NASJONAL DIGITAL LÆRINGSARENA

Vg2 IKT-servicefag

Fagstoff til eksamen

Innhold på ndla.no er nå tilgjengelig i PDF- eller ePub-format som hjelpemidler til eksamen. Disse filene kan lagres på egen datamaskin og leses i digitalt format, eller de kan skrives ut og tas med til eksamen. Dette er automatisk genererte filer som ikke er manuelt bearbeidet.

Dette dokumentet er en tekstutgave av det digitale læreverket for faget slik det forelå på ndla.no april 2015. For å se det komplette læreverket, slik det er sammensatt av ulike medietyper og interaktive elementer, gå til http://ndla.no.

Ved eksamen vil man ikke ha adgang til Internett, og dermed vil i hovedsak kun tekst og bilder være tilgjengelig. Animasjoner, simuleringer, lydfiler og video er interaktive ressurser som krever tilkobling til nett.

Sentralt gitt skriftlig eksamen i Kunnskapsløftet følger to hovedmodeller for hjelpemidler. I modell 1 er alle hjelpemidler tillatt. Unntak er Internett og andre verktøy som tillater kommunikasjon. For norsk og fremmedspråkene er heller ikke oversettelsesprogrammer tillatt.

Modell 2 er en todelt eksamen. Der er det i del 1 tillatt med skrivesaker, passer, linjal og vinkelmåler. I del 2 er alle hjelpemidler tillatt med unntak av Internett eller andre verktøy som tillater kommunikasjon.

Disse fagene følger modell 2 for hjelpemiddelbruk uten forberedelsesdel; matematikk i grunnskolen, matematikk i grunnskoleopplæringen for voksne, matematikk, fysikk, kjemi og biologi i videregående opplæring.

Innholdsfortegnelse

Innholdsfortegnelse 2

Bruker- og driftsstøtte 8

Etikk 8

Hva er personvern? 8

Personvernprinsippene 10

Personopplysningsloven 13

Datatilsynet 15

Innsynsretten 17

Meldeplikt 19

Konsesjonsplikten 20

Datalagringsdirektivet 22

Overvåking av ansattes bruk av IKT-systemer 23

Arbeidsgivers rett til innsyn i ansattes e-post og dokumenter 26

Framgangsmåten når en ansatts e-post eller dokumenter må åpnes 29

Hvordan håndtere e-post når ansatte slutter? 30

Hva skal du gjøre hvis du oppdager noe straffbart? 31

Publisering av personopplysninger om ansatte på Internett 32

Etiske problemer 33

Regelverk 35

Lover og regler for IKT-systemer 35

Krav til tilrettelegging og medvirkning 37

Krav til det fysiske arbeidsmiljøet 39

Universell utforming av IKT 41

Åndsverkloven 43

Regler for offentlige anskaffelser 45

Dokumentasjon av brukerstøtte 46

Innledning til hvordan brukerstøttefunksjonen er organisert og fungerer 46

Hva er en helpdesk? 47

Organisering av en helpdesk 49

Helpdeskprogramvare 52

Online helpdesk og automatisert helpdesk 54

Outsourcing av brukerstøtte 56

Oppgaver 57

Praktisk drift av helpdesk 57

Brukerstøtte 58

Serviceinnstilling 58

Video - Bruk av IKT i et serviceyrke 59
Kunnskaper og egenskaper 60
Hva forventes av en IKT-medarbeider? 63
Urealistiske forventninger til IKT-medarbeidere 65
Møte med brukerne 68
Kommunisere med brukere 70
Brukernes kunnskapsnivå 71
Datavegring 73
Feilsøkingsmetodikk 75
Driftsstøtte 79
Organisering av driftsstøtte 79
Sikkerhetskopiering 80
Vedlikeholds- og oppdateringsplaner 82
Kapasitetsplanlegging 84
Driftsavtaler og serviceavtaler 86
Fagterminologi 87
Kurs 88
Planlegging og gjennomføring av enkle kurs 88
Kartlegge opplæringsbehovet 90
Bestemme opplæringsform, kursinnhold og omfang 91
Lage informasjon om kurset 93
Holde kurset 94
Alternativer til kurs 96
Evaluere og følge opp kurset 97
Noen vanlige feil ved planlegging og gjennomføring av kurs 98
Oppgaver 99
Presentasjon av selvvalgt tema innen IKT 99
Kursplanlegging 100
Kunnskapsnettverk 101
Innledning til kunnskapsnettverk og kunnskapsutvikling 101
Personlige og profesjonelle læringsnettverk 102
Bygge et personlig læringsnettverk 103
Kunnskapsnettverk i virksomheter 105
RSS 106
Oppgaver 108
Skap et personlig læringsnettverk 108
Lag en digital CV 109
Hjelp og veiledning 110

Informasjonskilder 110
Internett som supportressurs 112
Feilsøking med søkemotor 113
Informasjon på egne nettsider – Ofte stilte spørsmål 117
Windows hjelpfunksjon 119
Windows feilsøkere 121
Windows fjernhjelp 123
Dokumentasjon og tilgjengeliggjøring 127
Hvorfor du må dokumentere 127
Dokumentere løsninger på problemer 128
Dokumentere rutiner 130
Skrive brukerdokumentasjon 132
Skrivetips 134
Skrive for skjerm 136
Skrive prosedyrer 138
Distribuere informasjon 140
Behovet for oppdateringer 142
Oppgaver 143
Rutinebeskrivelse 143
Informasjon for skjerm 144
Skrive brukerinformasjon 145

Drift og vedlikehold 146
Plan for systeminstallasjoner 146
Planlegge en systeminstallasjon 146
Planlegge den fysiske nettverksinstallasjonen 149
Planlegge sikkerhet 150
Nettverksdiagram 151
Beregne kostnadene for installasjonen 152
Planlegge utrulling og fallback 154
Program- og maskinvare 157
Innhente tilbud og anskaffe utstyr 157
Installere programvare og maskinvare 159
Liten nettverksinstallasjon 160
Funksjoner i et IKT-system 162
Dokumentere en systeminstallasjon 162
Hvorfor dokumentere? 164
Planlegg dokumentasjonen 165

Hva skal du dokumentere? 166
Automatisert dokumentasjon 168
Kostnadskontroll 170
Budsjettere investerings- og driftskostnader 170
Kostnad eller investering? 172
IKT-innkjøp 174
Drift og vedlikehold 176
Driftsoppgaver og daglig vedlikehold 176
Servervedlikehold 178
Vedlikeholdsplan 181
Driftsavtaler og serviceavtaler 183
Krav 184
Tilgjengelighet eller sikkerhet? 184
Databruk i endring og sikkerhetsbevisste brukere 186
Sikre soner 188
Vurdere risiko og konsekvenser 189
Tre typer sikkerhet 191
Fysisk sikkerhet 192
Driftssikkerhet 193
Feiltolerante systemer 194
RAID-løsninger 195
Avbruddsfri strømforsyning 197
Datasikkerhet 198
Sikkerhetskopiering 199
Utstyr for sikkerhetskopiering 201
Differensiell og inkrementell sikkerhetskopiering 203
Sikkerhetskopiering med rotasjon av lagringsmedier 205
Sikker sletting av data 207
IKT og HMS 210
Krav til utstyr for en dataarbeidsplass 212
Databriller 214
Datautstyr og miljø 215
Sikkerhet 217
Innledning til forebygging av sikkerhetsbrudd 217
Holde Windows pc-er oppdatert 219
Holde Apple Mac-maskiner oppdaterte 223
Oppdatering av andre programmer 226
Passord 228

Behandle passord 230
Datakryptering 234
Datavirus 238
Demilitariserte soner 240
Phishing – nettfisking 241
Identitetstyveri 245
Sikkerhet utenfor virksomheten 247
Data i skyen 249
Anmelde sikkerhetsbrudd 251
Sikkerhetsorganisasjoner 252
Oppgaver 254
Krypteringsaktivitet 254
Fagbegreper 256
Fagspråk 256
Norsk eller engelsk? 258
Når skal du ikke bruke fagspråk? 259

Virksomhetsstøtte 261

Kostnads- og nytteverdi 261
Dokumentere IKT-bruk 261
Kapasitetsovervåking 263
Vurdere kostnader og nytteverdi 1 264
Vurdere kostnader og nytteverdi 2 266
Økt kompleksitet gir økte kostnader 268
Kravdefinisjon 270
Innledning til IKT-støtte i arbeidsprosesser 270
Å lage et prosessflytdiagram 272
Identifisere roller i prosessen 275
Vurdere behovet for IKT-støtte 277
Kravdefinisjon og kravspesifikasjon 279
Oppgaver 281
Flytskjema med iterasjon 281
Vareleveringsvirksomheten 282
Planlegging 283
Litt om prosjektorganisering 283
Hva er spesielt for IKT-prosjekter? 284
Hvorfor IKT-prosjekter mislykkes 286
Vellykkede IKT-prosjekter 288

Innhente informasjon 290
Fokuser på virksomheten 292
Anskaffelser 293
Lover og regler når et nytt system skal tas i bruk 293
Personvern 294
Arbeidsmiljø 295
Universell utforming av IKT 296
Universell utforming av IKT / fagstoff 296
Åndsverkloven 297
Brukerundersøkelse 298
Undersøke brukertilfredshet 298
Utforme spørreskjema 301
Spørsmålstyper 303
Gjennomføre undersøkelsen 306
Analysere resultatene av undersøkelsen 308
Oppgaver 311
Brukerundersøkelse 311
Kontorstøttesystemer 312
Hva er kontorstøttesystemer? 312
Betingelser for effektivisering 314
Kontorstøttesystemer og nye rutiner 316
Opplæring 318
Kostnader 319
Kostnader 320
Totale eierkostnader 320
Totale eierfordeler 323
Innsparinger gir ikke alltid lavere kostnader 325
Behovskartlegging 327
Innledning til analyse av brukerstøtte 327
Analysere brukerstøtte 329
Konsekvenser 331
Oppgaver 333
Eksamensoppgaver 333
Eksamensoppgave 1 333

Bruker- og driftsstøtte

Etikk

Hva er personvern?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hva er personvern? (101577)

Personvern kan enkelt beskrives som retten til et privatliv og retten til å bestemme over egne personopplysninger. I en jobb som IKT-servicemedarbeider må du vite hvilke lover og regler som gjelder for personvern, fordi du kan komme i situasjoner der det er du som skal registrere, behandle eller ta vare på andres personopplysninger.

Det er flere lover som gjelder personvern. Den viktigste er personopplysningsloven, men noen yrkesgrupper har også egne lover og regler som må følges, som for eksempel helseregisterloven og regler om taushetsplikt.

– Hysj!

Fotograf: Jan Johannessen

Utgangspunktet for personvern er at alle har rett til et privatliv og rett til å bestemme hva andre skal kunne vite om deg og dine personlige forhold.

Men personvernet har også grenser. Noen ganger er samfunnets interesser viktigere enn det enkelte menneskets rett til personvern.

Som privatperson bør du selvsagt vite hvilke rettigheter du har, og hvordan personopplysninger om deg behandles. Og som IKT-servicemedarbeider må du vite hvilke lover og regler som gjelder for registrering og behandling av personopplysninger, slik at du ikke bryter andre menneskers rettigheter.

Det betyr at du må vite

- hvilke personopplysninger det er lov å registrere
- hvem som har lov til å registrere personopplysninger
- hvem som skal ha tilgang til personopplysninger
- hvordan personopplysninger skal lagres og beskyttes
- hvilken rett en person har til å få vite hva som er registrert
- hvilken rett en person har til å få endret eller slettet personopplysninger

Lenke: Hva er personvern?

I en jobb som IKT-servicemedarbeider må du vite hvilke lover og regler som gjelder for personvern, fordi du kan komme i situasjoner der det er du som skal registrere, behandle eller ta vare på andres personopplysninger.

Personvernprinsippene

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Personvernprinsippene (101580)

Personvernet bygger på noen grunnleggende prinsipper som kalles personvernprinsippene. Siden vi nå er inne på juss, kan språket og ordene som brukes, virke vanskelige. Men prinsippene er ikke vanskelige å forstå.

Personvernprinsippene er de grunnleggende reglene personvern skal baseres på. Prinsippene er:

- samtykke
- proporsjonalitet
- formålsbestemthet
- relevans og minimalitet
- fullstendighet og kvalitet
- informasjon og innsyn
- sikkerhetssensitive opplysninger

Samtykke

Samtykke betyr ganske enkelt at du skal være enig i og gi tillatelse til at personinformasjon om deg kan registreres. Samtykke skal i størst mulig grad være frivillig, uttrykkelig og informert.

At samtykket skal være informert, betyr at du har forstått hva det er du gir tillatelse til, og hvilke konsekvenser det eventuelt får for deg.

At samtykket er frivillig, betyr at du ikke skal bli presset til å gi tillatelsen.

At samtykket skal være uttrykkelig, betyr at du må gjøre noe aktivt for å gi tillatelse. For eksempel ved å sende inn en svarslipp, krysse av på et skjema eller svare positivt på et spørsmål.

Proporsjonalitet

Proporsjonalitet betyr at informasjonen ikke skal brukes til noe annet enn det den ble samlet inn for, eller på en måte som går ut over den som er registrert.

Formålsbestemthet

Formålsbestemthet betyr at det må være en grunn til at personopplysningene samles inn.

Relevans og minimalitet

Relevans betyr at personopplysninger bare skal registreres når det er absolutt nødvendig, og minimalitet betyr at det bare er den informasjonen som er nødvendig, som skal registreres. Hvis det ikke lenger er bruk for informasjonen, skal den slettes.

Fullstendighet og kvalitet

Fullstendighet og kvalitet betyr at personopplysningene skal være fullstendige, riktige og oppdaterte.

Informasjon og innsyn

Informasjon betyr at du skal bli informert når noen registrerer personinformasjon om deg, og at du skal vite hva personopplysningene brukes til. Innsyn betyr at du har rett til å se hva som er registrert om deg, og få mulighet til å rette feil eller slette gale opplysninger.

Informasjonssikkerhet

Informasjonssikkerhet betyr at de som oppbevarer personopplysningene, må sørge for at opplysningene ikke blir ødelagt, og at ingen uvedkommende får tilgang til dem.

Sensitive opplysninger

Sensitive opplysninger er personopplysninger som er svært personlige, eller som lett kan misbrukes. Som sensitive opplysninger regnes etnisk opphav, politiske meninger, religiøs overbevisning, medlemskap i fagforeninger, opplysninger om helse eller seksualliv, og om man har vært mistenkt, siktet eller straffet for et lovbrudd. For registrering av slike opplysninger gjelder spesielt strenge regler, og i utgangspunktet er det ikke lov til å registrere dem i det hele tatt.

En persons seksuell legning er sensitiv informasjon og skal ikke registreres.

Fotograf: Espen Braata

Anonymitet

Anonymitet innebærer at hvis det ikke er nødvendig å kunne identifisere den som har gitt opplysninger, har man rett til å være anonym. Når for eksempel et firma eller et meningsmålingsbyrå gjennomfører en spørreundersøkelse, skal de bare registrere svarene på spørsmålene, og ikke hvem som har svart på undersøkelsen.

Lenke: Personvernprinsippene

Lenke: Samtykke

Sensitive opplysninger er personopplysninger som er svært personlige, eller som lett kan misbrukes. For eksempel etnisk opphav, politiske meninger, religiøs overbevisning, medlemskap i fagforeninger og opplysninger om helse og seksualliv. For registrering av slike opplysninger gjelder spesielt strenge regler, og i utgangspunktet er det ikke lov til å registrere dem i det hele tatt.

Personopplysningsloven

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Personopplysningsloven (101585)

Personopplysningsloven er den viktigste loven om personvern i Norge. I den står reglene for hva det er lov til å registrere om privatpersoner, og hvordan personopplysninger skal behandles.

Datamaskiner brukes til registrering og lagring av alle typer opplysninger, og personopplysninger blir rutinemessig registrert i mange offentlige og private dataregister.

Myndighetene registrerer for eksempel alle innbyggere i Norge i folkeregisteret. Hvis du har inntekt, er du registrert i skatteregisteret. Hvis du tar opp studielån, blir du registrert hos Lånekassen. Når du tar førerkort og kjøper en bil, blir du registrert i førerkortregisteret og kjøretøyregisteret. Alle trygdede er registrert i trygderegisteret, og så videre.

Hver eneste norske borger blir utstyrt med hvert sitt registreringsnummer. Personnummersystemet ble i sin tid utarbeidet av Statistisk Sentralbyrå og innført fra 1. januar 1967.
Fotograf: Bjørn Finstad

Også bedrifter og ulike institusjoner har personregister. Banker, forsikringsselskap, foreninger, skoler, arbeidsgivere, politiske partier eller trossamfunn man er medlem av, registrerer informasjon om sine kunder, ansatte og medlemmer. I tillegg kommer selvsagt alle register som benyttes i markedsførings- og reklamesammenheng.

For å forhindre at registrert informasjon om privatpersoner blir misbrukt, eller at det registreres informasjon som er feil eller svært personlig, har Stortinget vedtatt lov om behandling av personopplysninger. Vanligvis blir den bare kalt personopplysningsloven.

Personopplysningsloven er den viktigste loven om personvern i Norge. I den står reglene for hva det er lov til å registrere, og hvordan personopplysninger skal behandles. Loven gjelder for både bedrifter og offentlig sektor, men ikke for opplysninger som privatpersoner registrerer for personlige eller private formål.

Personopplysningsforskriften

I tillegg til personopplysningsloven er det også laget en forskrift til loven kalt personopplysningsforskriften. Mens loven slår fast prinsippene for hva som er lov, og hva som ikke er lov, forklarer forskriften hvordan reglene skal gjennomføres i praksis.

Det finnes flere lover og regler som IKT-medarbeidere må være oppmerksomme på. Selv om du bør forvente at en arbeidsgiver vet hvilke lover som gjelder for IT-systemer på en arbeidsplass, er det slett ikke alltid tilfelle at vedkommende gjør det. Du må derfor ha et bevisst forhold til hva de systemene du har ansvaret for brukes til, hvilken informasjon som lagres, og hvem som har tilgang til informasjonen.

Lenke: Personopplysningsloven

Lenke: Personopplysningsforskriften

> Personopplysningsloven er den viktigste loven om personvern i Norge. I den står reglene for hva det er lov til å registrere om privatpersoner, og hvordan personopplysninger skal behandles.

Datatilsynet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datatilsynet (101591)

Datatilsynets oppgave er å overvåke at personopplysningsloven overholdes.

For å passe på at personopplysningsloven overholdes, har myndighetene opprettet et eget uavhengig tilsyn kalt Datatilsynet.

Fordelene med at Datatilsynet er uavhengig, er at heller ikke regjeringen, departementene eller politikere kan styre eller gjøre om de beslutningene Datatilsynet tar. Dermed kan Datatilsynet også passe på at heller ikke myndighetene registrerer personopplysninger de ikke har lov til å registrere.

Datatilsynets oppgaver er

- å kontrollere at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet
- å holde seg orientert om nasjonal og internasjonal utvikling når det gjelder behandling av personopplysninger
- å identifisere farer for personvernet og gi råd om hvordan farene kan unngås eller begrenses
- å være høringsinstans i saker som berører personvern
- å delta i råd og utvalg, bistå bransjeorganisasjoner med å gi råd og utarbeide normer for å sikre personopplysninger i virksomhetene
- å stimulere til opprettelse av personvernombud og bygge kompetanse hos ombudene
- å ha en ombudsrolle mot publikum og gi råd og informasjon
- å få viktige saker på dagsorden i media og bidra til samfunnsdebatt om personvern

Lenke: Datatilsynets oppgaver

Datatilsynet er et uavhengig tilsyn som skal overvåke at personopplysningsloven overholdes. Ingen kan styre eller overprøve de beslutningene Datatilsynet tar.

Datatilsynet og SlettMeg.no jobber aktivt med saker der bilder har blitt publisert på Facebook eller lignende, uten at den som er på bildet, har samtykt.
Fotograf: Roger Neumann

Innsynsretten

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innsynsretten (101593)

Et viktig prinsipp i personopplysningsloven kalles innsynsretten. Innsynsretten betyr at alle har rett til å få vite hvilke personopplysninger som er registrert om dem, hvorfor opplysningene er registrert, og hva de brukes til.

Innsynsretten er enkeltpersoners rett til å få vite hva som er registrert om dem i personregister. I praksis betyr det at alle har krav på å få en utskrift av de opplysningene som er registrert om dem, når de ber om det. Denne retten gjelder overfor alle typer virksomheter, organisasjoner og offentlige institusjoner.

Når den som eier registeret, får en henvendelse om innsyn, må han levere opplysningene senest innen 30 dager. Registereieren har heller ikke lov til å ta betalt av den som ber om innsyn.

Hvis det viser seg at registeret inneholder personopplysninger som er

- uriktige
- ufullstendige
- foreldede
- ulovlige å registrere (for eksempel sensitive opplysninger)

må den som eier registeret, rette eller slette det som er feil.

For rene adresseregister som brukes til for eksempel reklameutsendinger, kan du kreve å få navnet ditt slettet fra registeret. Firmaet som eier registeret, må da gjøre det så snart som mulig.

Det finnes unntak

Det finnes imidlertid enkelte unntak fra innsynsretten. Den gjelder ikke for register som bare brukes til statistikk, forskning eller generelle planleggingsformål. Et godt eksempel er Statistisk sentralbyrås register.

Statistisk sentralbyrå (SSB) har lov til å registrere opplysninger som skal brukes til forskning på og planlegging av norske samfunnsforhold. SSB publiserer resultatene av arbeidet sitt og formidler det blant annet til politikere og allmennheten.

Fotograf: Heiko Junge

Det er også unntak for opplysninger som det kan ha alvorlige konsekvenser for en persons helse, eller for personer som står en nær, å få tilgang til. I praksis vil dette vanligvis gjelde opplysninger som kan føre til at en helsesituasjon forverres, eller at det kan være fare for selvmord.

Et annet eksempel er politiets register, der det kan finnes informasjon om hvem som har gitt politiet informasjon om en forbrytelse.

Til slutt er det gjort unntak for register som inneholder informasjon som gjelder rikets sikkerhet. Overvåkingspolitiets register og militære register er eksempler på slike.

Når den som eier registeret, får en henvendelse om innsyn, må han eller hun levere opplysningene senest innen 30 dager. Registereieren har heller ikke lov til å ta betalt av den som ber om innsyn.

Meldeplikt

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Meldeplikt (101596)

Registrering av personopplysninger som ikke er sensitive, må meldes til Datatilsynet. Men det finnes mange unntak.

Når en virksomhet ønsker å registrere og bruke personopplysninger som ikke er sensitive, må de si fra til Datatilsynet senest 30 dager i forveien.

Meldingen er bare en informasjon til Datatilsynet. Så lenge man overholder personregisterloven, kreves det ikke noen egen tillatelse for å opprette et personregister, men Datatilsynet skal vite om det. På Datatilsynets nettsider ligger det et eget skjema som skal brukes.

Melding om behandling av personopplysninger

Skjema for melding om behandling av personopplysninger etter personopplysningsloven §31 og helseregisterloven §29.

Side: 1/1

1. Meldingen gjelder

a)
- Melding etter personopplysningsloven
- Melding etter helseregisterloven

b)
- Førstegangsregistrering av melding/gjenregistrering av melding etter tre år
- Endring av melding nr: _____ med meldingsnøkkel: _____

c)
Planlagt oppstart for behandlingen av personopplysninger (dd.mm.åååå): _____

2. Sensitive personopplysninger

Gjelder meldingen sensitive personopplysninger?
- Ja
- Nei

Oppbevares opplysningene kun i et manuelt personregister?
- Ja
- Nei

3. Kontaktopplysninger - den behandlingsansvarlige virksomheten

Meldeskjema for behandling av personopplysninger

Legg spesielt merke til at skjemaet inneholder en egen del med kontaktopplysninger for den personen som er behandlingsansvarlig. Behandlingsansvarlig er den personen som skal ha ansvaret for at personopplysningsloven overholdes.

Selv om hovedregelen er at alle personregister skal meldes inn til Datatilsynet, finnes det en del unntak for vanlige registre. Kunde- og leverandørregister, abonnementsregister, medlemsregister i foreninger og lignende er ikke meldepliktige.

Et viktig unntak for IKT-servicemedarbeidere er aktivitetslogger i datasystemer og nettverk. For å kunne administrere og sørge for sikkerhet i et nettverk, er det ofte behov for å logge informasjon om bruk og trafikk som kan spores tilbake til enkeltpersoner. Men den informasjonen som samles inn, skal bare brukes til administrasjon og sikkerhetstiltak.

Lenke: Melding og konsesjon

Konsesjonsplikten

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Konsesjonsplikten (101598)

Den som skal registrere sensitive personopplysninger, må ha en egen tillatelse fra Datatilsynet.

For å opprette og bruke et personregister som inneholder sensitive opplysninger, må man først få tillatelse fra Datatilsynet. En slik tillatelse kalles en konsesjon.

Sensitive personopplysninger er opplysninger om

- politisk, filosofisk eller religiøs oppfatning
- rase, hudfarge eller etnisk opprinnelse
- at en person har vært mistenkt, siktet, tiltalt eller dømt for straffbare forhold
- fysisk eller psykisk helsetilstand
- seksuell legning eller andre seksuelle forhold
- medlemskap i fagforeninger

Sensitive opplysninger – som soning av fengselsstraff – skal behandles på en slik måte at de ikke kan misbrukes.
Fotograf: Stein J. Bjørge

På Datatilsynets nettsider ligger det et eget skjema som skal brukes for å søke om konsesjon.

Lenke: Konsesjonsskjema

Datatilsynet har rett til å kontrollere at konsesjonen overholdes, og kan kreve å få adgang til alle personregister og datamaskiner som brukes til disse. De kan også gjennomføre kontroll der de mener det er nødvendig. Denne retten er ikke begrenset av bestemmelser om taushetsplikt, som noen yrkesgrupper er underlagt.

Lenke: Melding og konsesjon

Datalagringsdirektivet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datalagringsdirektivet (101600)

Datalagringsdirektivet trådte i kraft den 1. juli 2012 og påbyr tele- og internettleverandører å lagre alle trafikkdata.

Datalagringsdirektivet (DLD) er et EU-direktiv som påbyr alle tele- og internettleverandører i Norge å lagre trafikkdata, lokaliseringsdata og abonnementsdata i 6 måneder for alle som bruker telefon, mobiltelefon, e-post og Internett.

Stort serverrom
Fotograf: Corbis

Det vil si opplysninger om hvem som kommuniserer med hvem, når kommunikasjonen fant sted, hvor de kommuniserende befant seg, og hvilken kommunikasjonsform som ble benyttet.

Hensikten er at politiet skal ha tilgang til disse opplysningene ved etterforskning og straffeforfølging av alvorlig kriminalitet.

Lenke: Datalagringsdirektivet

Overvåking av ansattes bruk av IKT-systemer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Overvåking av ansattes bruk av IKT-systemer (101603)

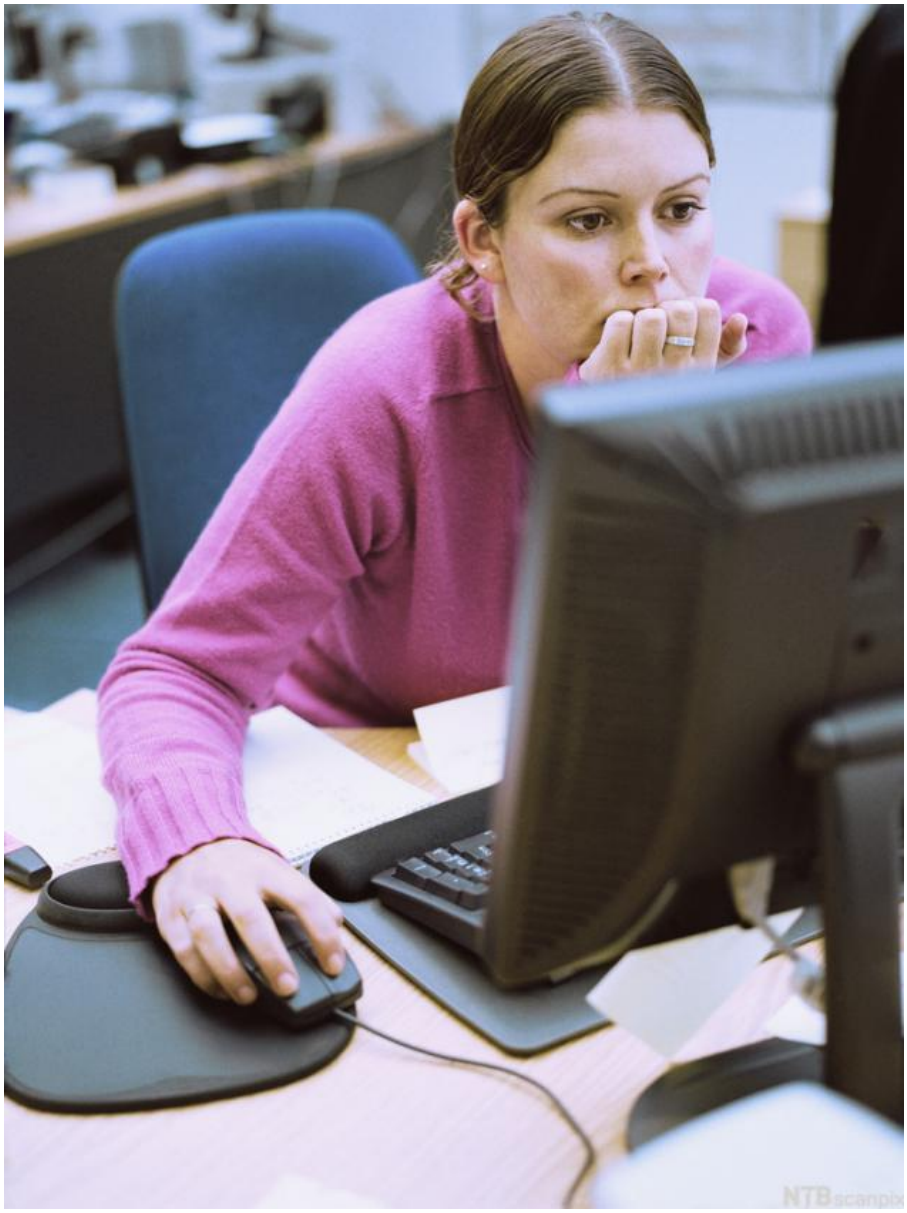
Datasystemer og nettverk gir arbeidsgivere mulighet til å overvåke ansattes bruk av virksomhetens datamaskiner, men det er regler for hva det er lov til å overvåke, og hvordan det skal gjøres.

De fleste datasystemer har mulighet for automatiske loggfunksjoner, og det er ofte nødvendig av sikkerhetshensyn.

Det er derfor lov til å registrere hvem som har forsøkt å logge seg på, og om det ble godtatt eller ikke. Det er også vanlig å logge hvem som til enhver tid bruker ulike filer og program, internettaktivitet og utskrifter.

Slike logger kan brukes til systemadministrasjon og sikkerhet, men hvis virksomheten vil bruke informasjonen til noe annet, må den først få samtykke fra de ansatte.

De fleste virksomheter har regler for hva det er lov til å bruke virksomhetens datamaskiner og nettverk til. For eksempel at det ikke er lov til å laste ned musikk eller filmer, installere program, surfe på bestemte typer nettsider eller bruke maskinen til private formål.



Det kan av og til være fristende å bruke arbeidstiden til å surfe på nettet.

Fotograf: Helen King

Arbeidsgiver kan overvåke at reglene ikke brytes, men overvåkingen skal skje på gruppenivå og ikke på personnivå. Det vil si at arbeidsgiver skal kunne få se om reglene brytes, men ikke hvem som bryter dem.

Arbeidsgiveren skal så gi de ansatte beskjed om at det vil bli kontrollert hvem som bryter reglene, hvis aktiviteten ikke opphører innen en gitt frist. Hvis regelbruddene fortsetter, kan arbeidsgiver bruke loggene til å finne ut hvem som står bak, uten samtykke fra de ansatte.

Arbeidsgiveren kan ikke uten videre kartlegge hvor mye tid hver enkelt ansatt bruker på Internett, eller hvilke internettsider som blir besøkt. Loggene kan for eksempel ikke benyttes til overvåking av de ansatte til bruk ved oppsigelser. Slik bruk av loggopplysninger skal meldes til Datatilsynet.

Siden det er IKT-medarbeidere som vanligvis er ansvarlig for systemlogger og skal utføre selve overvåkingen, er det viktig at du kjenner disse reglene godt, og vet hva du kan og ikke kan gjøre.

Lenke: Kan arbeidsgiveren overvåke det arbeidstakeren gjør på Internett?

Arbeidsgivers rett til innsyn i ansattes e-post og dokumenter

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Arbeidsgivers rett til innsyn i ansattes e-post og dokumenter (101604)

De fleste ansatte i en virksomhet disponerer en egen datamaskin og har en egen e-postadresse på jobben. Det skaper problemer når arbeidsgiveren har behov for tilgang til data som ligger på maskinen, eller e-post som er sendt til den ansattes e-postadresse.

De fleste arbeidsgivere synes det er greit at de ansatte kan bruke virksomhetens datamaskiner til enkelte private gjøremål. De fleste benytter derfor maskinen til både jobbrelaterte og private gjøremål.

Noen ganger oppstår det situasjoner der arbeidsgiver ønsker å kontrollere hva den ansatte bruker datamaskinen til, eller har behov for tilgang til informasjon som ligger på maskinen eller den ansattes e-postkonto. Eksempler kan være når

- den ansatte er borte fra jobben på grunn av sykdom eller ferie og arbeidsgiver har behov for å kontrollere at ikke e-posthenvendelser til bedriften blir liggende ubesvart
- den ansatte er borte fra jobben og arbeidsgiver har behov for dokumenter som ligger på den ansattes maskin
- det er mistanke om at arbeidstakeren opptrer illojalt, for eksempel ved å gi opplysninger videre til konkurrerende selskap
- det er mistanke om at arbeidstakeren bruker datamaskinen til noe som er ulovlig eller i strid med bedriftens regler

For å unngå juridiske og etiske problemer må bedriften ha klare regler for bruk av datamaskiner og e-post til private formål på arbeidsplassen. Videre må man forsikre seg om at de ansatte er gjort kjent med reglene. Reglene må også si noe om i hvilke situasjoner de ansatte må akseptere at arbeidsgiveren kan åpne e-postmeldinger eller filer som ligger på den enkeltes område på en arbeidsstasjon eller server.

Arbeidsgivers rett til innsyn

Arbeidsgiverens rett til innsyn i de ansattes e-post på jobben kan til en viss grad sammenlignes med arbeidsgiverens gjennomgang av innholdet i posthyllene til de ansatte. Det vil finnes situasjoner der arbeidsgiveren har en saklig grunn for å gå gjennom posthyllen for å se etter post som angår bedriften. For eksempel når ansatte er fraværende over lengre tid på grunn av ferie eller sykdom.

Ved for eksempel langtids sykefravær kan det være nødvendig for arbeidsgiver å sjekke e-posten til den ansatte slik at henvendelser fra kunder o.l. ikke blir liggende ubesvart.
Fotograf: Corbis

Det samme gjelder for den ansattes e-postkasse. E-postkasser skiller seg imidlertid fra vanlige posthyller ved at det er vanskeligere å skille private meldinger fra de som gjelder jobben. Arbeidsgiveren bør derfor be om samtykke til å se i e-postkassa før den ansatte drar på ferie eller mens vedkommende er sykemeldt.

Et annet problem er at det i mange e-postlesere ofte benyttes automatisk forhåndsvisning. Dermed kan arbeidsgiveren uforskyldt lett komme til å se mer informasjon enn det han i utgangspunktet har behov for eller rett til.

Private e-poster

Bedriften kan lage regler som sier at datamaskiner bare skal brukes til jobbrelaterte formål, men arbeidsgiver har likevel ikke lov til å lese all e-post de ansatte mottar. Grunnen til dette er at de ansatte ikke har noen mulighet til å styre hva som sendes til deres e-postkontoer på jobben.

Innholdet av meldinger som for eksempel sendes av venner eller familie, vil fortsatt være private, selv om de sendes til en e-postkonto som tilhører bedriften. Som hovedregel har ikke arbeidsgiveren rett til innsyn i åpenbart private e-postmeldinger eller filer, og han har heller ikke lov til å be om samtykke til slikt innsyn eller lage regler om dette.

Hvis virksomheten ikke ønsker at de ansatte skal motta privat post på bedriftens e-postkontoer, kan man lage regler som sier at alle slike meldinger skal slettes. Dette er imidlertid sjelden praktisk siden det ofte vil innebære at all innkommende e-post til bedriften må gjennomgås manuelt.

I tillegg tilsier vanlig høflighet at både mottaker og avsender får beskjed hvis en e-postmelding blir slettet. Det største problemet er imidlertid som oftest å avgjøre om en e-post eller en fil er privat eller virksomhetsrelatert, uten å åpne den.

Navn på e-postadresse

De fleste bedrifter benytter e-postadresser som angir den ansattes navn, initialer eller lignende i adressen, slik som *ola.nordmann@bedrift.no* eller *on@bedrift.no.* Dersom den ansatte logger seg på med eget brukernavn og passord, bør han kunne forvente at post til denne e-postkontoen ikke åpnes av andre enn han selv, med mindre annet er avtalt med arbeidsgiver på forhånd.

E-postadresser av typen *henvendelse@bedriften.no* eller *salgsavdelingen@bedriften.no* framstår som klart virksomhetsrelatert. Verken avsender eller mottaker av e-post til en slik adresse vil kunne forvente at den skal behandles som privat post. Dette kan imidlertid være mer tvilsomt hvis avsenderen har merket e-posten med en navngitt ansatt eller har skrevet «konfidensielt» eller lignende i emnefeltet. I slike tilfeller anbefaler Datatilsynet å spørre den ansatte før andre eventuelt åpner den.

En mulig løsning på problemene med å skille ut privat e-post er å la de ansatte ha to e-postadresser. For eksempel *ola.nordmann@bedriften.no* og *ola.nordmann.privat@bedriften.no*. Rutiner for å merke private e-postmeldinger og filer med «privat», eventuelt plassere disse i egne mapper, vil også kunne hjelpe. Men det er ikke noen garanti for at det ikke oppstår problemer.

Framgangsmåten når en ansatts e-post eller dokumenter må åpnes

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Framgangsmåten når en ansatts e-post eller dokumenter må åpnes (101605)

Arbeidsgivere har ofte behov for å åpne en ansatts e-post eller dokumenter, men det kommer lett i konflikt med personvernet.

Arbeidsgiveren kan noen ganger ha et saklig behov for å åpne en ansatts e-post eller dokumenter. Dersom det er laget regler for slike situasjoner, og de ansatte er klar over disse, er det tilstrekkelig til at arbeidsgiveren kan åpne e-poster og dokumenter som angår virksomheten. Hvis det ikke finnes slike regler, må den ansatte gi samtykke først.

Selv om det er laget regler, er det viktig at den ansatte blir informert på forhånd om at e-post eller dokumenter blir åpnet. Hvis den ansatte er tilgjengelig, bør han få anledning til å være til stede og eventuelt sortere ut hvilke e-postmeldinger og dokumenter som er private.

Dersom den ansatte ikke er tilgjengelig, er det viktig at vurderingen av om opplysningene er private, gjøres før e-posten eller dokumentet åpnes. Dersom det ser ut som det er privat, skal det ikke åpnes. Noen ganger kan det likevel skje at man vurderer feil og ved et uhell åpner noe som viser seg å være privat. Da skal filen snarest lukkes. I tillegg bør den ansatte i etterkant få vite hva som ble åpnet.

Tastatur.

Fotograf: Jon Eeg

Hvordan håndtere e-post når ansatte slutter?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hvordan håndtere e-post når ansatte slutter? (101606)

Ansatte som slutter, kan være et problem fordi virksomheten har behov for å motta e-post som sendes til en tidligere ansatts e-postadresse.

Når en ansatt slutter, bør vedkommendes e-postadresse slettes slik at ikke privat e-post sendes til virksomheten. Et problem som ofte oppstår i denne sammenhengen, er virksomhetens behov for å motta e-post som sendes til en tidligere ansatts e-postadresse.

For å unngå å komme i konflikt med personvernet og reglene for innsyn i e-post kan dette løses ved at all e-post til den aktuelle adressen slettes automatisk, kombinert med at det sendes en melding om at vedkommende ikke lenger er ansatt i bedriften, og en ny e-postadresse for henvendelser som gjelder bedriften.

Det er ikke en god løsning å videresende e-post fra en tidligere ansatts e-postadresse til en annen person i virksomheten, siden eventuell privat e-post også vil bli videresendt.

Virksomheten har imidlertid anledning til å inngå en avtale med den tidligere ansatte om at e-postadressen beholdes i en begrenset periode, eventuelt med videresending til en ny adresse.

> Når en ansatt slutter, bør arbeidsgiveren slette vedkommendes e-postadresse slik at privat e-post ikke sendes til virksomheten.

Hva skal du gjøre hvis du oppdager noe straffbart?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hva skal du gjøre hvis du oppdager noe straffbart? (101607)

Hvis du oppdager at datautstyr eller nettverk brukes til noe som er straffbart, skal politiet alltid varsles.

En arbeidsgiver er ansvarlig for at virksomhetens datautstyr ikke brukes til noe ulovlig. Hvis du mistenker at noen bruker virksomhetens datautstyr eller nettverk til for eksempel å formidle barnepornografi eller annet ulovlig materiale, skal det alltid anmeldes og overlates til politiet.

Ved mistanke om for eksempel underslag eller spredning av barnepornografi eller lignende tar politiet beslag i pc-er og lagringsmedier.
Fotograf: Luca Kleve-Ruud

I slike tilfeller skal du ikke starte noen egen «etterforskning». Da risikerer du å ødelegge bevis hvis du åpner filer eller e-post uten at det er tatt nødvendige forholdsregler.

Isteden bør du varsle arbeidsgiver og forsøke å sikre logger, maskiner, brukerkontoer og eventuelle lagringsområder på servere på en forsvarlig måte inntil politiet kan overta.

Hvis du har en mistanke om at datautstyr eller nettverk brukes til noe straffbart, skal du varsle politiet og ikke starte noen egen «etterforskning».

Publisering av personopplysninger om ansatte på Internett

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Publisering av personopplysninger om ansatte på Internett (101608)

En virksomhet har lov til å legge ut enkelte opplysninger om de ansatte på Internett. Men opplysningene som legges ut, må gjelde arbeidsforholdet.

En virksomhet har lov til å legge ut enkelte opplysninger om de ansatte på sine nettsider, facebooksider eller lignende. Men opplysningene som legges ut, må gjelde arbeidsforholdet. Det er for eksempel lov til å publisere navn, stilling, ansvarsområder, telefonnummer og e-postadresse hos bedriften for de ansatte uten samtykke.

Hvis man også vil legge ut bilder av de ansatte, må de det gjelder, samtykke til dette først. Det samme gjelder dersom arbeidsgiveren ønsker å publisere privatadresser eller andre mer detaljerte opplysninger om arbeidstakeren, slik som alder, sivilstand eller cv.

På intranett (lukkede lokalnett) kan bedriften i tillegg legge ut bilder av de ansatte uten først å innhente samtykke. Men bildene må fjernes hvis arbeidstakeren ber om det. Publisering av bilder fra firmafester og lignende skal først skje etter samtykke fra de som er gjenkjennelige på bildene.

Virksomheten har lov til å legge ut informasjon som gjelder arbeidsforholdet til sine ansatte, på Internett. For eksempel navn, stilling, ansvarsområder, telefonnummer og e-postadresse.

Etiske problemer

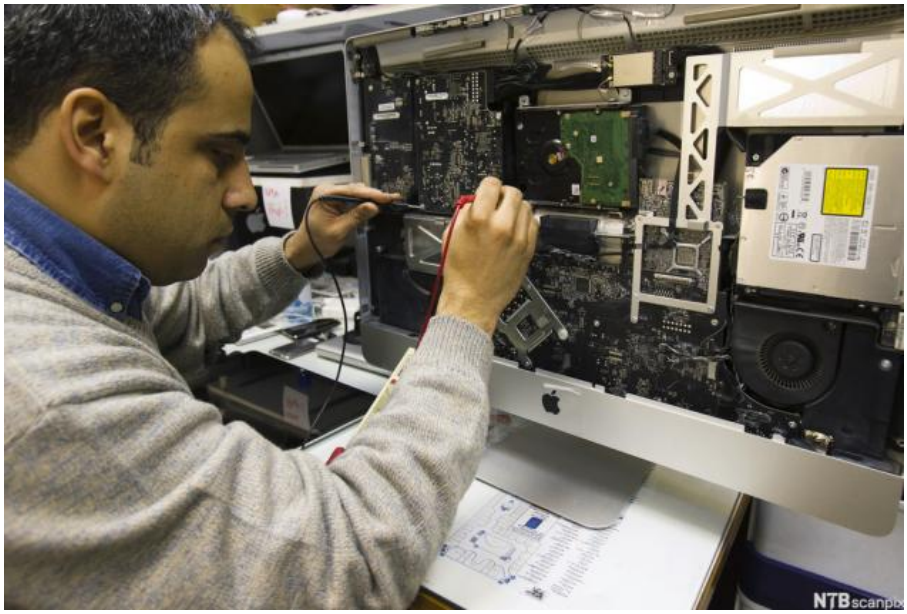
Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Etiske problemer (101609)

Etiske problemer innebærer gjerne at du kommer i en lojalitetskonflikt, og ofte er det ikke noen «riktig» løsning på problemet.

En spesiell type problemer du kan komme ut for i jobben som IKT-servicemedarbeider, er hvordan du skal forholde deg til informasjon du egentlig ikke skulle hatt tilgang til.

IKT-medarbeidere har ofte administrative rettigheter og dermed adgang til informasjon som egentlig er konfidensiell. Dette kan være informasjon som bedriften betrakter som intern, men det kan også være sensitive persondata, avhengig av hvilken type virksomhet du arbeider for. Informasjon som lagres på datamaskinene ved et advokatkontor eller legesenter, vil for eksempel kunne være svært sensitiv.

I mange tilfeller er virksomheten avhengig av at IKT-servicemedarbeiderne er til å stole på, og at de er i stand til å håndtere konfidensiell eller sensitiv informasjon på en forsvarlig måte. Virksomheten har få kontrollmuligheter med hvilken informasjon IKT-medarbeideren får tilgang til.



Husk at du som IKT-medarbeider må håndtere sensitive opplysninger – også bedriftshemmelige opplysninger – på riktig måte når IT-utstyr for eksempel sendes ut av bedriften for reparasjon.
Fotograf: RAHEB HOMAVANDI

Som IKT-servicemedarbeider må du også være oppmerksom på denne problematikken hvis utstyr må sendes til ekstern service, eller hvis det kommer eksterne teknikere eller konsulenter. Det kan for eksempel være nødvendig å fjerne harddisken i en maskin før den sendes til service, av hensyn til den informasjonen som ligger der.

I tillegg til den informasjonen som virksomheten lagrer om sin egen drift, sine kunder eller klienter, brukes ofte datamaskinen på jobben også til mer private gjøremål som brevskriving, internettsurfing og privat e-post. Det kan derfor finnes svært mye informasjon som du i utgangspunktet ikke skulle hatt tilgang til.

Etiske dilemma

I de fleste tilfeller er tilgang til konfidensiell eller privat informasjon ikke noe problem. Så lenge du ikke gjør noe ulovlig eller uetisk, skader du ingen. Problemet oppstår når du av en eller annen grunn oppdager informasjon som setter deg i et etisk dilemma. Det vil si at du blir usikker på hva som er riktig å gjøre.

Det finnes ingen «oppskrift» på hvordan du bør håndtere etiske dilemma, og det finnes ofte ikke noen helt riktig løsning på slike problemer. Det betyr selvsagt ikke at det er likegyldig hvordan du handler. Et etisk dilemma krever som oftest at du tenker nøye gjennom konsekvensene av de valgene du har, og det er ofte en fordel å diskutere saken med en utenforstående du stoler på. Forutsetningen er selvsagt at dette ikke kan skape ytterligere problemer.

Typisk for etiske dilemma er at du kommer i en lojalitetskonflikt overfor arbeidsgiver, kollegaer eller myndigheter. Hvis du for eksempel oppdager at en kollega har søkt jobb hos en konkurrent, vil lojalitet til virksomheten og arbeidsgiveren tilsi at du opplyser ledelsen om dette. Samtidig vil lojaliteten til kollegaen tilsi at du ikke sier noe.

Det beste er selvsagt å unngå å sette seg selv i en slik situasjon. Du må ha et bevisst forhold til informasjon som er av privat eller konfidensiell karakter, og unngå å lese den, selv om det kan være aldri så fristende. Hvis du likevel kommer i en situasjon der du oppdager noe som kan skape en konfliktsituasjon, bør du la vedkommende som er ansvarlig for informasjonen, få vite dette, slik at du gir han en mulighet til selv å rydde opp i situasjonen eller avklare eventuelle misforståelser.

Du må ha et bevisst forhold til informasjon som er av privat eller konfidensiell karakter, og unngå å lese den, selv om det kan være aldri så fristende.

IKT-servicemedarbeider (interaktiv) / flashnode
http://ndla.no/nb/node/105018

Regelverk

Lover og regler for IKT-systemer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Lover og regler for IKT-systemer (101704)

Det finnes flere lover og regler som direkte eller indirekte angår bruken av IKT-systemer, og som IKT-medarbeider må man være oppmerksom på disse. Selv om du bør kunne forvente at arbeidsgiveren vet hvilke lover som gjelder, er det ikke alltid tilfelle at vedkommende gjør det.

I tillegg til reglene som gjelder personvern, finnes det også lover og avtaler som skal sikre at arbeidstakere ikke «overkjøres» av datateknologi på arbeidsplassen. Den viktigste av disse er **arbeidsmiljøloven**.

En virksomhet må også passe på at den ikke bryter **åndsverkloven,** og at de ansatte ikke bruker virksomhetens nettverk til å laste ned rettighetsbeskyttet materiale (piratkopiering).

I 2013 kommer det nye regler for **universell utforming** av IKT. Universell utforming betyr at et IKT-system skal kunne brukes av alle – også av dem som har en funksjonshemning.

Nettstedet The Pirate Bay ble startet i 2003. Tjenesten gjør det mulig å overføre store mengder data og har både lovlige og ulovlige bruksområder. De ansvarlige ble i 2009 dømt til ett års fengsel og fikk en bot på 30 millioner kroner.
Fotograf: Claudio Bresciani

Krav til tilrettelegging og medvirkning

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Krav til tilrettelegging og medvirkning (101705)

I arbeidsmiljøloven er det en egen paragraf som sier at arbeidstakerne har krav på å bli informert og å delta i planleggingen når en virksomhet skal endre systemer som brukes i arbeidet. Paragrafen nevner ikke datamaskiner og IKT-systemer spesielt, men det er ofte i den sammenhengen den er aktuell.

Utgangspunktet i arbeidsmiljøloven § 4–2 er at arbeidstakerne skal bli løpende informert om systemer som brukes i arbeidet, at de får nødvendig opplæring i bruk av systemene, og at de skal være med når de blir utformet.

Paragrafen stiller fem krav:

1. Det skal legges til rette for at arbeidstakeren gis mulighet for faglig og personlig utvikling gjennom arbeidet sitt.
2. Arbeidet skal organiseres og tilrettelegges med hensyn til den enkeltes arbeidsevne, kunnskaper, alder og andre forutsetninger.
3. Det skal legges vekt på mulighet til selvbestemmelse, innflytelse og faglig ansvar.
4. Det skal gis mulighet for variasjon og for å se sammenheng mellom enkeltoppgaver.
5. Det skal gis nok informasjon og opplæring til at arbeidstakeren er i stand til å utføre arbeidet når det skjer endringer i vedkommendes arbeidssituasjon.

I praksis betyr dette at når en virksomhet skal gjøre endringer i IKT-systemene sine, må de informere de ansatte på forhånd og gi alle som blir berørt av endringene, mulighet til å uttale seg. Loven er aktuell bare når endringene har betydning for hvordan den enkelte skal gjøre jobben sin, og gjelder ikke vanlige oppgraderinger av program og lignende.

Når nye systemer skal tas i bruk, må de som skal bruke dem, få nok opplæring til at de klarer å gjøre jobben og forstå hva de gjør.

Opplæring i ny programvare er svært viktig for at de ansatte skal føle seg trygge og raskt bli kompetente.
Fotograf: Corbis

Man må også ta hensyn til hvilke forutsetninger den enkelte har. Et godt eksempel er en virksomhet som innfører et nytt avansert datasystem som skal brukes av personer som har liten eller ingen erfaring med IKT fra før. Da kreves det naturlig nok mye opplæring.

Lenke: Arbeidsmiljøloven

Arbeidstakere har rett til å bli informert og være med i planleggingen av nye IKT-systemer på arbeidsplassen.

Krav til det fysiske arbeidsmiljøet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Krav til det fysiske arbeidsmiljøet (101706)

Arbeidsmiljøloven har strenge regler for å sikre at arbeidstakere ikke blir skadet eller syke av jobben.

I utgangspunktet skulle man ikke tro at personer som jobber ved en datamaskin er særlig utsatt for skader eller sykdom, men det er et par ting du må passe på.

I § 4–4 i arbeidsmiljøloven står det at arbeidsplassen skal innredes og utformes slik at arbeidstakerne unngår uheldige fysiske belastninger, og at nødvendige hjelpemidler skal stilles til disposisjon.

En person som bruker mesteparten av arbeidsdagen foran en dataskjerm, kan få problemer med stiv nakke og stive skuldre, ryggproblemer og senebetennelse i armen, ofte kalt musearm.

Feil belastning over lang tid ved bruk av mus kan gi store muskel- og skjelettplager.
Fotograf: Mikkel Østergaard

Mye av fraværet på norske arbeidsplasser skyldes muskelplager på grunn av ensformig arbeid foran dataskjermen. Det er derfor viktig at arbeidsplassen utformes på en slik måte at man unngår unødige belastninger.

Du må også passe på at ikke datamaskiner eller skrivere som støyer mye, plasseres i rom der noen skal sitte og jobbe.

Lenke: Musearm

Lenke: Arbeidsmiljøloven

IKT-arbeidsplasser må utformes på en slik måte at unødige belastninger unngås.

Universell utforming av IKT

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Universell utforming av IKT (101707)

Universell utforming av IKT handler om å utforme IKT-løsninger slik at de kan brukes av alle – uavhengig av funksjonsnivå.

Universell utforming betyr at noe skal kunne brukes av alle, også av dem som har en funksjonshemning, som for eksempel bevegelseshemning, dårlig syn eller dårlig hørsel.

Fornyings-, administrasjons- og kirkedepartementet har utarbeidet en forskrift med krav til universell utforming av IKT-løsninger. Planen er at en slik utforming skal bli lovpålagt fra 2013, men innholdet i kravene blir ikke endelig kjent før forskriften trer i kraft.

I første omgang skal reglene om universell utforming gjelde for nettløsninger og automater, slik at alle skal kunne bruke dem. Det kan for eksempel være billettautomater, minibanker, netthandelssider, nettsider med informasjon til allmennheten og lignende.

I praksis betyr reglene at nettsteder som faller inn under forskriften, for eksempel må ha funksjoner som gjør at tekst kan leses med talesyntese. Talesyntese betyr at man kan be datamaskinen om å lese teksten på skjermen høyt.

Enkle hjelpemidler, som hodesett, kan gjøre arbeidet foran pc-en mer komfortabelt for ansatte som for eksempel ønsker å benytte talesyntese på nettsider.
Fotograf: Harry Maynard

Reglene skal ikke gjelde for sosiale medier som blogger, Facebook, Twitter og andre tjenester som brukes i privat sammenheng.

Lenke: Universell utforming av IKT

Universell utforming av IKT-løsninger betyr at de skal kunne brukes av alle – uavhengig av funksjonsnivå.

Åndsverkloven

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Åndsverkloven (101708)

Åndsverkloven sier at alle former for kopiering og nedlasting av rettighetsbeskyttet materiale er forbudt når man er klar over eller burde forstå at materialet er gjort tilgjengelig på ulovlig måte.

Stortinget vedtok våren 2005 endringer i åndsverkloven som gjør at alle former for kopiering og nedlasting av rettighetsbeskyttet materiale er forbudt når man er klar over eller burde forstå at materialet er gjort tilgjengelig på ulovlig vis – såkalt piratkopiering. Dette inkluderer musikk, film, tekster (bøker), bilder og programvare.

Selv om det er den enkeltes ansvar å overholde loven, bør virksomheter ta forholdsregler for å unngå ulovlig nedlasting fra internett, for eksempel ved å blokkere bestemte typer filer og nettsteder og ved å inkludere regler for dette i bedriftens interne retningslinjer for bruk av IKT-systemer.

Virksomheten må selvsagt også passe på at de har gyldige lisenser for all programvare som brukes av de ansatte i jobben.

Et annet vanlig problem er at ansatte finner bilder på Internett som de kopierer og bruker i virksomhetens presentasjoner, brev, brosjyrer, nettsider og så videre. Mange er ikke klar over at dette er brudd på åndsverkloven, og virksomheten må derfor informere de ansatte om det.

Dersom du vil bruke et bilde i presentasjoner, på nettsider eller i andre publikasjoner, må du passe på at du faktisk har lov til å bruke det aktuelle bildet.
Fotograf: Anette Karlsen

Lenke: Åndsverkloven

Virksomheter kan blokkere for bestemte typer filer og nettsteder for å unngå ulovlig nedlasting.

Regler for offentlige anskaffelser

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Regler for offentlige anskaffelser (101709)

De fleste private bedrifter og organisasjoner står helt fritt når de skal velge IKT-systemer, leverandører og samarbeidspartnere. I det offentlige er det imidlertid mange regler som må følges.

Med det offentlige mener vi alle etater, organer, direktorat, kontor og foretak i stat, fylkeskommune og kommune.

Vi har regler for offentlige anskaffelser for at alle skal kunne ha tillit til at offentlige penger blir brukt på en samfunnstjenlig måte. Reglene skal

- sikre rettferdig konkurranse mellom leverandører til det offentlige
- sørge for at staten får mest mulig igjen for pengene sine
- hindre at noen får fordeler på grunn av familieforhold, vennskap eller lignende

Norge er dessuten internasjonalt forpliktet gjennom EØS-avtalen og WTO-avtalen til å følge bestemte framgangsmåter ved større offentlige anskaffelser.

Det er lett å forstå at dette er viktig, når vi vet at det offentlige årlig bruker nesten 400 milliarder kroner på kjøp av varer og tjenester, bygg og anlegg.

Fire hovedprinsipper

Reglene for offentlige anskaffelser er basert på fire hovedprinsipper:

- **likebehandling**, som betyr at alle leverandører skal få samme betingelser, krav og muligheter
- **forutsigbarhet**, som betyr at alle deler av anskaffelsesprosessen skal være forutsigbar for leverandørene, slik at det ikke dukker opp noen overraskelser etterpå
- **gjennomsiktighet**, som skal sikre at det er mulig å kontrollere at alle regler blir fulgt
- **konkurranse**, som skal sikre at statens penger og ressurser brukes mest mulig effektivt

Reglene gjelder for alle typer anskaffelser av varer og tjenester, uavhengig av verdi.

Når du arbeider som IKT-medarbeider i det offentlige, kan du altså ikke bare bestille det du trenger av utstyr, programvare eller tjenester uten videre. Alle bestillinger må vanligvis gå gjennom en innkjøpsansvarlig som kjenner reglene for offentlige anskaffelser.

Lenke: Regelverk for offentlige anskaffelser

Lenke: Lov om offentlige anskaffelser

Dokumentasjon av brukerstøtte

Innledning til hvordan brukerstøttefunksjonen er organisert og fungerer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innledning til hvordan brukerstøttefunksjonen er organisert og fungerer (102150)

Virksomheter investerer i datasystemer for å bli mer effektive. Mange virksomheter er så avhengige av datasystemene sine at de ansatte i praksis blir sittende uten å kunne gjøre noe hvis systemene ikke fungerer som de skal.

Datasystemer som ikke fungerer, kan medføre store kostnader i form av tapt arbeidstid, tapt salg, forsinkelser, irriterte kunder og så videre. Det er derfor viktig at brukerne får hjelp når de trenger det, og at problemer løses raskt.

Virksomheter som har en ineffektiv brukerstøtte eller forsøker å spare penger på brukerstøtte, ender ofte opp med å tape mer enn de sparer. Når brukerne ikke får hjelp eller ikke har tillit til at IKT-medarbeiderne kan hjelpe dem, vil de heller forsøke å løse problemene på egen hånd eller finne andre måter å utføre oppgavene sine på, selv om det tar lengre tid og resultatet blir dårligere.

Å organisere en effektiv og godt fungerende brukerstøtte er derfor en god investering for de fleste virksomheter.

Noen virksomheter velger å ha én eller flere IKT-medarbeidere som jobber med brukerstøtte, og som brukerne kan kontakte når de har problemer. En annen mulighet er å organisere brukerstøtten som en **helpdesk.**

Virksomheter som forsøker å spare penger på brukerstøtte, ender ofte opp med å tape mer enn de sparer.

Hva er en helpdesk?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hva er en helpdesk? (102151)

Betegnelsen «helpdesk» brukes ofte om alle former for brukerstøtte eller kundestøtte, men helpdesk er egentlig en måte å organisere brukerstøtte på.

I utgangspunktet var helpdesken en skranke som kunder kunne henvende seg til for å få hjelp, eller et telefonnummer de kunne ringe. Helpdesken ble derfor ofte også kalt «callsenter». Etter hvert som alle har fått tilgang til Internett, er online-løsninger og automatisert brukerstøtte blitt vanlig. Du vil også kunne støte på betegnelser som «supportsenter», «responssenter», «kundesenter» og lignende.

En enkel definisjon av helpdesk er:

«En helpdesk er et sentralt punkt der problemer og feil rapporteres inn, registreres, administreres og løses.»

I sin enkleste form er en helpdesk bare et telefonnummer, en e-postadresse, en nettside eller en skranke, der det er noen som tar imot henvendelser og forsøker å løse problemer. På mange skoler, for eksempel, drives en slik brukerstøttetjeneste av elever med IKT-kompetanse.

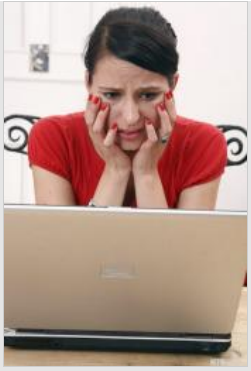
Det vesentlige er at kundene og brukerne har ett enkelt kontaktpunkt for alle spørsmål eller problemer de måtte ha med IKT.

En helpdesk kan enten være intern for virksomhetens egne ansatte (brukerstøtte) eller ekstern for virksomhetens kunder (kundestøtte). Uansett er hensikten med å opprette en helpdesk å organisere støtten på en mest mulig effektiv måte. Målet er å utnytte ressursene best mulig for

- å redusere responstiden (tiden det tar fra en bruker melder fra om et problem, til noen begynner å arbeide med å løse problemet)
- å redusere servicetiden (tiden det tar fra noen begynner å arbeide med problemet, til det er løst)
- å minimalisere kostnadene til brukerstøtte

Helpdesk er egentlig en egen måte å organisere brukerstøtte på. Dette er imidlertid ikke alltid like klart for alle, og du vil derfor kunne støte på betegnelsen «helpdesk» brukt om vanlig brukerstøtte, selv om den ikke er organisert som en helpdesk.

En helpdesk er et sentralt punkt der problemer og feil rapporteres inn, registreres, administreres og løses.



For å unngå at de ansatte kaster bort mye tid på selv å forsøke å løse IKT-problemer, bør bedriften ha en godt fungerende helpdesk.
Fotograf: Mike Schröder

Organisering av en helpdesk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Organisering av en helpdesk (102152)

Helpdesk er en egen måte å organisere brukerstøtte på, selv om du ofte vil oppleve at alle typer brukerstøtte kalles for helpdesk.

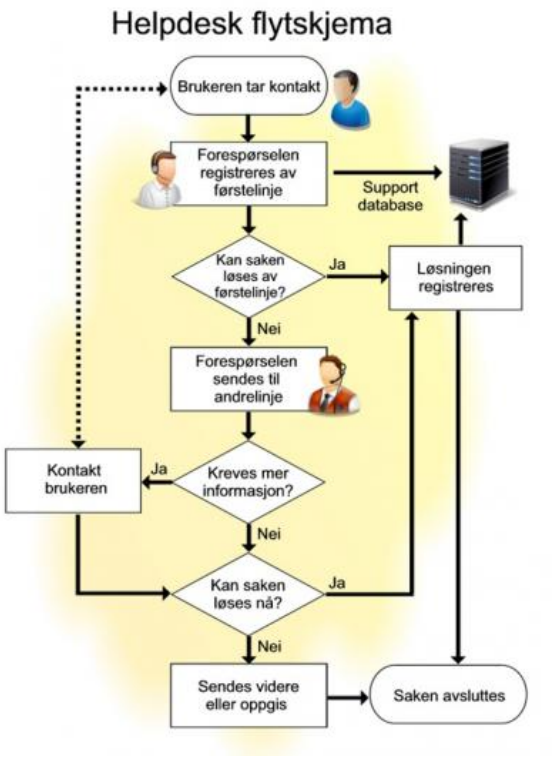
En helpdesk er ofte organisert i to nivåer. Første nivå (ofte kalt førstelinje) er IKT-medarbeidere som tar imot spørsmål fra brukerne, mens neste nivå (kalt andrelinje) er teknikere, systemeksperter eller andre med mer spesialisert kunnskap.

Legg spesielt merke til at vi snakker om brukerstøtte som en prosess. Noe av det viktigste med å opprette en helpdesk er å gjøre brukerstøtten **prosessdrevet** i stedet for **personavhengig**.

Med det menes at brukerstøtte ikke skal være avhengig av enkeltpersoner i bestemte stillinger.

Dette er en vesentlig forskjell fra vanlig brukerstøtte eller en IKT-avdeling, som typisk vil være personavhengig.

Et eksempel på helpdeskprosessen er illustrert i flytskjemaet under:



Helpdesk

Opphavsmann: Arne Jansen

Brukeren tar kontakt

Prosessen starter med at kunden eller brukeren tar kontakt med helpdesken for å få hjelp med et problem eller svar på et spørsmål. Dette kan skje via telefon, Internett, e-post, personlig frammøte eller på annen måte. Det vesentlige for brukeren er at han eller hun har ett enkelt kontaktpunkt uansett hva henvendelsen gjelder. Dette er også vesentlig for virksomheten.

Uansett hvilken måte brukeren velger for å kontakte brukerstøtte, skal henvendelsen alltid gå gjennom helpdesken. Ideelt sett skal det ikke være mulig for en bruker eller kunde å få svar på spørsmål eller hjelp med et problem uten først å kontakte helpdesken.

Forespørselen blir registrert

Førstelinje har ansvaret for å registrere alle henvendelser. Dette gjøres uansett om problemet kan løses med en gang, eller om det må sendes videre. Å registrere alle henvendelser er viktig fordi en helpdesk er prosessdrevet og ikke persondrevet. Det betyr at ansvaret for å følge opp henvendelser og løse problemer er lagt til stillinger og ikke til personer. Brukerne skal kunne være sikre på at alle henvendelser blir behandlet, uavhengig av om enkeltpersonene som bemanner helpdesken, blir syke, har ferie eller slutter i jobben. Når en ny medarbeider overtar en stilling, skal vedkommende enkelt kunne se hva som er gjort tidligere.

Å registrere alle henvendelser er også viktig for ressursplanleggingen, ved at man kan ta ut nøyaktig statistikk over hvilke typer problemer og henvendelser helpdesken mottar.

Førstelinje løser problemet eller sender det videre

Førstelinje kontrollerer så om problemet kan løses med en gang. Personen som tar imot forespørselen, vil ha tilgang til en supportdatabase der forslag til løsning på alle vanlige problemer er registrert.

Hvis problemet ikke kan løses med en gang av førstelinje, blir det overført til andrelinje. Hvis denne er tilgjengelig, kan brukeren settes over med en gang, men i mange tilfeller vil brukeren få beskjed om at han eller hun blir kontaktet. Dette gir dem som er ansvarlige for brukerstøtte, mulighet for å prioritere og fordele oppgavene slik at ressursene utnyttes på best mulig måte. De som arbeider i andrelinje, blir ikke forstyrret av telefoner eller forespørsler og kan konsentrere seg om de sakene de arbeider med.

Legg også merke til at førstelinje ikke skal bruke for lang tid på å forsøke å løse et problem. Førstelinje skal bare ta seg av de problemene som er kjent, og som kan løses raskt. Typisk vil dette være vanlige brukerfeil. Det er ikke førstelinjes oppgave å feilsøke eller forsøke å løse mer kompliserte problemer. Det kan føre til at tilgangen til helpdesken blir blokkert, slik at responstiden blir lang.

Andrelinje vurderer om man har tilstrekkelig informasjon

Når andrelinje mottar saken, vurderer de om den informasjonen som er registrert av førstelinje, er tilstrekkelig for å løse saken. Hvis det er behov for mer informasjon, kontaktes brukeren igjen, og manglende informasjon innhentes.

Det kan også være behov for å kontakte andre leverandører for å innhente informasjon fra dem.

Andrelinje løser problemet

Andrelinje vurderer nå hvilke ressurser som må settes inn for å løse problemet, og begynner å arbeide med saken. Avhengig av hvilke ressurser man har til disposisjon, kan dette inkludere fjernsupport, besøk hos brukeren/kunden eller annet. Når problemet er løst, blir løsningen registrert i supportdatabasen, og saken avsluttes.

Hvis problemet ikke kan løses, blir det overført til neste ledd (tredjelinje) hvis det finnes. Dette kan for eksempel være leverandørens supportsenter eller en spesialist.

I noen tilfeller er det umulig eller ikke hensiktsmessig å løse problemet. Det kan for eksempel bli uforholdsmessig dyrt, eller utstyret lar seg ikke reparere.

Noe av det viktigste med å opprette en helpdesk er å gjøre brukerstøtten prosessdrevet i stedet for personavhengig.

Helpdeskprogramvare

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Helpdeskprogramvare (102157)

Brukerstøtte og helpdesk er helt avhengig av gode IKT-systemer og rutiner for å fungere effektivt.

Gode systemer for registrering og gjenfinning av informasjon er en svært viktig del av brukerstøtte- og helpdeskoppsettet. Systemene må sørge for

- at alle forespørsler blir registrert, fulgt opp og løst
- at alle løsninger og all kunnskap lagres og kan gjenfinnes hurtig
- at det er mulig å ta ut detaljerte rapporter og statistikk for vurdering og planlegging

Det finnes en rekke programpakker som er utviklet spesielt for ivareta disse kravene.

Husk at *alle* henvendelser til helpdesken skal registreres.
Fotograf: Lise Åserud

Alle forespørsler må registreres, uansett om de kan løses med en gang eller ikke.

Alle forespørsler må registreres, følges opp og løses

Alle forespørsler må registreres. Selv om problemet kan løses av førstelinje umiddelbart, er det viktig for planleggingen at også de sakene som ikke krever noen videre behandling, er registrert i systemet.

Det kan også være nyttig for den som tar imot forespørselen, å kunne se den enkelte brukerens eller kundens forhistorie. Har vedkommende for eksempel hatt samme eller tilsvarende problem tidligere?

Når forespørselen er registrert, må systemet sørge for at den blir fulgt opp. I et prosessdrevet system ønsker man ikke å være avhengig av at enkeltpersoner skal huske hva som er gjort, eller hva som skal gjøres.

Hver henvendelse som ikke løses i førstelinje, merkes derfor med dato/klokkeslett og gis gjerne en prioritet før den sendes videre til andrelinje. Systemet fungerer deretter som et styringsverktøy ved at det forteller dem som arbeider i andrelinje, hvilke oppgaver som står for tur.

Hvis en oppgave ikke er påbegynt eller løst innen en bestemt tidsfrist, vil systemet varsle om dette og eventuelt justere opp prioriteten. Systemet kan også varsle når brukeren eller kunden skal kontaktes igjen for oppfølging, uavhengig av om saken er løst eller ikke. I en del systemer har man også automatiserte tilbakemeldinger, slik at det automatisk sendes en e-post til kunden eller brukeren med en beskjed om status etter en gitt tid.

Alle som er involvert i saken, vil registrere hva de gjør, slik at man til enhver tid kan gå inn og se hva som er gjort, hvem som har ansvaret, når kunden ble fulgt opp, og når saken forventes å bli løst.

Alle løsninger og all kunnskap må lagres og være mulig å finne igjen hurtig

Kunnskapsdatabasen står sentralt i helpdesksystemet og er det viktigste verktøyet for hurtig problemløsing. I basen registreres løsningen på alle problemer og feil etter hvert som de dukker opp. Kunnskapsdatabasen kan være frittstående, men ofte vil den også være koblet til kundedatabasen i et CRM-system (Customer Relations Management – kundeoppfølgingssystem), slik at det er mulig å se hvilke produkter kunden har kjøpt, og hvilke andre avdelinger/personer vedkommende har vært i kontakt med.

Det må være mulig å ta ut statistikk for vurdering og planlegging

I tillegg til å sørge for at alle forespørsler blir fulgt opp, er den informasjonen man får ut i form av statistikk, helt vesentlig for effektivisering og framtidig planlegging av helpdeskens arbeid. Et godt system vil kunne svare på spørsmål som for eksempel:

- Hvor mange forespørsler kommer det per dag?
- Hvordan fordeler belastningen seg per dag/uke/måned?
- Hvordan fordeler forespørslene seg på produkter?
- Hvor lang er gjennomsnittlig responstid?
- Hvor lang er gjennomsnittlig servicetid?
- Hvor mange forespørsler løses av førstelinje?
- Hvor mange forespørsler løses av andrelinje?
- Hvilken type problemer tar lengst tid å løse?
- Hvor mange forespørsler kan ikke løses?

Denne informasjonen gir virksomheten bedre styringsmuligheter for hvilken bemanning man har behov for, hvilke kunnskaper IKT-medarbeiderne må ha, og så videre.

I tillegg til systemet som ivaretar hovedfunksjonene (registrering, oppfølging, kunnskap og statistikk), kommer eventuelle andre programprodukter som medarbeiderne må ha tilgang til. Dette kan være de programmene brukerne har på sine maskiner, programvare for fjernsupport og lignende.

Online helpdesk og automatisert helpdesk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Online helpdesk og automatisert helpdesk (102158)

Telefon er fortsatt den vanligste måten for å kontakte helpdesken, men online helpdesker og automatiserte helpdesker er gode alternativer.

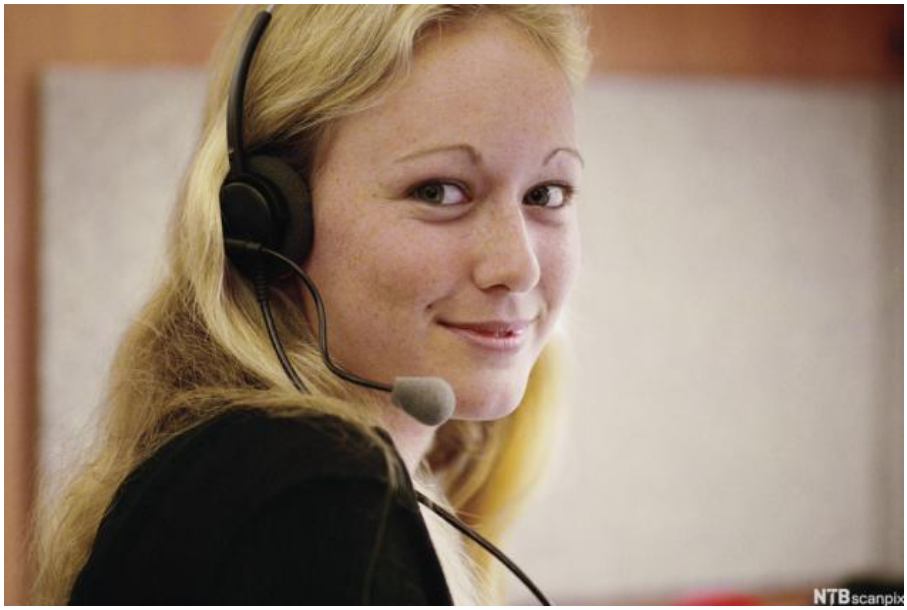
Før Internett var telefon den eneste praktiske måten å håndtere forespørsler på, og en helpdesk ble derfor ofte betegnet som et «callsenter». Selv om telefon fortsatt er en mulighet som foretrekkes av mange, har telefonsupport enkelte ulemper både for brukerne og for dem som drifter helpdesken.

Ulemper ved telefonsupport for kundene/brukerne:

- Brukerne/kundene blir frustrerte når de blir satt på venting, må navigere seg gjennom endeløse menysystemer eller stadig blir satt over til nye personer.
- Feil eller problemer kan normalt bare rapporteres inn i vanlig arbeidstid.
- Man får ikke nødvendigvis snakke med den som faktisk kan eller skal løse problemet.

Ulemper ved telefonsupport for helpdesken:

- Det kan være vanskelig å beregne hvor mange forespørsler som til enhver tid kommer. Det gjør at man noen ganger vil være overbemannet og andre ganger underbemannet. Det første innebærer en unødig kostnad, mens det andre fører til at brukerne/kundene ikke får svar eller blir satt i kø.
- Man må ofte ringe tilbake til brukeren flere ganger. Denne kostnaden belastes helpdesken.
- Alle forespørsler må registreres manuelt i supportdatabasen.



Å bruke telefonen til IKT-support har både fordeler og ulemper.

Fotograf: Corbis

Internett gjør at det er mulig å melde feil til en online helpdesk ved å fylle ut et feilmeldingsskjema på skjermen eller sende en e-post (noe som selvsagt er litt håpløst hvis problemet er at maskinen eller nettet ikke fungerer).

En online helpdesk fjerner flere av ulempene med hjelp over telefon. Brukerne kan rapportere feil hele døgnet, og man blir aldri satt i kø. For dem som driver helpdesken, er bemanningsproblemet mindre, og feilmeldinger kan registreres automatisk i supportdatabasen.

Automatisert helpdesk

Selv om en helpdesk som regel er kostnadsbesparende i forhold til vanlig brukerstøtte når supportvolumet blir stort nok, er det fortsatt store kostnader ved å drive en helpdesk.

Moderne databaseteknologi kombinert med Internett har ført til at stadig flere virksomheter ser på muligheten for å automatisere deler av brukerstøtten ved at brukeren selv finner fram til svaret på problemene sine.

Det finnes flere ulike systemer for automatisert hjelp, men de fleste er bygd opp rundt et system der maskinen stiller brukeren en rekke spørsmål om hva problemet består i, og deretter foreslår ulike løsninger i form av steg-for-steg-beskrivelser. Mange av de store programleverandørene har slike løsninger for de vanligste problemene brukerne har med programmene.

En online helpdesk fjerner flere av ulempene med hjelp over telefon. Brukerne kan rapportere feil hele døgnet, og man blir aldri satt i kø.

Outsourcing av brukerstøtte

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Outsourcing av brukerstøtte (102160)

Det er ikke alle virksomheter som ser det som en hovedoppgave å drive egen brukerstøtte, og mange er heller ikke store nok til å kunne opprette og drifte sin egen helpdesk.

Mange virksomheter velger derfor å sette bort (outsource) brukerstøtten til et firma som har spesialisert seg på dette. Fordelene ved en slik løsning ligger først og fremst i kostnadsreduksjoner ved at man ikke lenger behøver å lønne egne IKT-medarbeidere.

Å la et annet firma overta brukerstøtten er mulig ved å bruke programmer for fjernstyring av brukerens datamaskin. Brukeren starter et program på maskinen sin som gjør at en IKT-medarbeider kan se brukerens skjermbilde på sin maskin og overta styringen av mus og tastatur via Internett.

Selv om outsourcing kan bidra til å effektivisere brukerstøtten og redusere kostnadene i forhold til å ha egne IKT-medarbeidere, vil IKT-support fortsatt være en vesentlig budsjettpost.

Det er heller ikke alltid virksomheten oppnår de innsparingene de ønsker. Et annet firma mangler ofte kunnskap om virksomhetens særegenheter, mål og brukermønster. Det fører igjen til at det kan ta lengre tid å løse problemer som oppstår, at problemene ikke blir løst på den mest hensiktsmessige måten, eller at problemene prioriteres feil.

Det er blitt mer og mer vanlig å outsource ulike supportfunksjoner. På bildet ser vi et callsenter i utlandet, men også norske bedrifter påtar seg outsourcing-oppdrag. Fotograf: Corbis

Det er viktig at firmaet som overtar brukerstøtten, har kunnskap om virksomhetens særegenheter, mål og brukermønster.

Oppgaver

Praktisk drift av helpdesk

Forfatter: Jan Frode Lindsø
Praktisk drift av helpdesk (131031)

Spiceworks er en applikasjon som tilbyr ulike funksjoner for blant annet overvåkning av nettverksressurser med mer. Det er helpdesk-funksjonen av applikasjonen vi skal benytte i denne oppgaven.

Spiceworks er en applikasjon som tilbyr ulike funksjoner for blant annet overvåkning av nettverksressurser med mer. Det er helpdesk-funksjonen av applikasjonen vi skal benytte i denne oppgaven. Last ned Spiceworks gratis fra Spiceworks, eller bruk tilsvarende programvare.

Del 1. Oppsett og konfigurasjon (gruppe)

Dere skal, sammen i grupper på 3 elever, sette opp en server med Spiceworks-applikasjonen. Denne skal fungere slik at dere kan koble opp mot Spiceworks-serveren fra en ekstern PC som er i samme nettverk som serveren. Dere kobler til ved å bruke IP-adressen til serveren, og portnummeret som serveren benytter (standard er 9675), som for eksempel http://192.168.1.1:9675/. Det kan også være nødvendig å måtte åpne for trafikk i brannmuren.

Spiceworks skal konfigureres på en hensiktsmessig måte, og nødvendige brukere må legges inn.

Del 2. Brukerstøtte (individuelt/gruppe)

Når helpdesken er satt opp vil dere få forespørsler fra brukere. Dette kan være folk som trenger hjelp til alt fra enkle problemer, til mer avanserte. Det er også forskjellige nivå på de som kontakter dere. Lærere eller medelever kan opptre som disse brukerne.

Det er derfor viktig at dere kommer med gode og velformulerte løsninger på problemene. Dere må også vurdere riktig prioritering på henvendelsene, og husk at det er brukeren som avgjør om han/hun har fått et tilfredsstillende svar på sin henvendelse.

Del 3. Prøve/rapport (individuelt)

Etter at prosjektet er gjennomført skal dere svare på spørsmål knyttet til oppgaven.

1. Skriv litt om egne erfaringer, innsats, samarbeid og læring i forbindelse med prosjektet
2. Hvordan vil du definere en helpdesk?
3. Hvordan er brukerstøtte ofte organisert?
4. Hva kjennetegner en god IT-supportmedarbeider?
5. Hvilke tiltak ville du satt igang dersom du opplever at mange brukere har samme type feil?
6. Hvordan bør vi prioritere forskjellige saker?

Brukerstøtte

Serviceinnstilling

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Serviceinnstilling (102209)

IKT-brukerstøtte er et serviceyrke og krever at du har en positiv serviceinnstilling. Men hva er egentlig service, og hva innebærer det å være serviceinnstilt?

Oppfatningen av service er avhengig av hvilke forventninger du har på forhånd. Vi snakker ofte om at vi har fått god eller dårlig service, men dette er egentlig en subjektiv oppfatning som er avhengig av tidligere erfaringer, hva du er blitt lovet, og hva du mener du kan forvente i en gitt situasjon.

Hvis du har urealistiske forventninger, vil du oppfatte servicen som dårlig uansett hvor god den er. Motsatt vil selv helt enkel service oppfattes som god hvis du i utgangspunktet ikke har noen forventninger. To personer som får nøyaktig samme behandling, kan altså ha vidt forskjellig oppfatning av kvaliteten på den servicen de fikk.

For deg som IKT-servicemedarbeider betyr det at du først må etablere en realistisk oppfatning hos brukerne av hva som er akseptabel service – altså hva de bør forvente når det gjelder responstid, hjelp og servicetid, slik at du har mulighet til å yte service på et nivå som brukerne er fornøyd med.

Å være serviceinnstilt innebærer at du er bevisst på hvilke forventninger brukerne har til service, og at du anstrenger deg for å oppfylle disse forventningene. Det betyr ikke at du skal gi noen spesialbehandling eller finne deg i hva som helst, men at du skal gjøre ditt beste for at brukerne skal bli fornøyd med den servicen de får. Noen brukere vil alltid være mer krevende enn andre og må kanskje få litt ekstra service for å bli fornøyd. Det viktigste er at du viser at du er villig til å anstrenge deg for å hjelpe brukerne.

Om du har fått god eller dårlig service, er en subjektiv oppfatning som er avhengig av tidligere erfaringer, hva du er blitt lovet, og hva du mener du kan forvente.

Serviceinnstilling er svært viktig når du arbeider som IKT-servicemedarbeider. Fotograf: Peter Melander

Du bør imidlertid være forsiktig med å forskjellsbehandle brukere. Mennesker har en tendens til å bli misunnelige på hverandre også på en arbeidsplass, og hva slags datautstyr man får tildelt, kan gi grunnlag for slik misunnelse.

Video - Bruk av IKT i et serviceyrke

Forfatter: Hanne-Lisbet Løite
Bruk av IKT i et serviceyrke (140708)

Hva er egentlig service, og hva innebærer det å være serviceinnstilt? Denne videoen tar for seg oppgavene til en IKT-servicemedarbeider med utgangspunkt i et virkelig problem. Eksempler på god service presenteres på en engasjerende og troverdig måte.

Bruk av IKT i et serviceyrke / video
http://ndla.no/nb/node/134714

Kunnskaper og egenskaper

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kunnskaper og egenskaper (102216)

Det er fort gjort å tro at det bare er de tekniske kunnskapene som er avgjørende for en IKT-medarbeider. Jobben går jo tross alt ut på å løse IKT-tekniske problemer. Faktum er imidlertid at du trenger en rekke andre egenskaper og ferdigheter for å kunne gjøre en god jobb.

Vi kan dele inn behovet for kunnskap og egenskaper i to hovedkategorier: spesielle og generelle. De spesielle er de som gjelder den tekniske kunnskapen om maskiner og program, mens de generelle er alle de ferdighetene og egenskapene som kreves for å kunne yte service på en god måte.

Spesielle kunnskaper

- tekniske kunnskaper om IKT
- kunnskaper om spesifikke systemer og program

Generelle kunnskaper og egenskaper

- evne til å prioritere
- evne til å administrere oppgaver
- evne til å håndtere stressituasjoner
- evne til å arbeide selvstendig
- evne til å tenke systematisk
- evne til å kunne kommunisere godt skriftlig og muntlig
- evne til å løse problemer
- tålmodighet
- serviceinnstilling

På skolen vil det ofte dreie seg mest om de spesielle kunnskapene, men for en arbeidsgiver er de generelle egenskapene minst like viktige.

Uansett hvor teknisk flink du er, er det til liten nytte hvis du ikke er i stand til å bruke kunnskapene dine i en arbeidssituasjon.

La oss se nærmere på de generelle egenskapene som kreves av en IKT-medarbeider. Merk at punktene på lista er satt opp i tilfeldig rekkefølge, og at ingen av egenskapene er viktigere enn de andre.

Myten om nerden som kan alt om datamaskiner, men som ikke er i stand til å få seg en jobb, er ikke bare fri fantasi.
Fotograf: Matthias Ritzmann

Evne til å prioritere

Du må ha god kunnskap om den virksomheten du arbeider i, og de målene den forsøker å nå, for å kunne prioritere de ulike oppgavene på en slik måte at det som er viktigst, blir gjort først.

Når oppgavene står i kø og alt tilsynelatende haster, blir det fort slik at den som roper høyest, får hjelp først. Men det er slett ikke sikkert at dette er i virksomhetens interesse. Hvis du ikke kjenner bedriften godt, kan du bli usikker på hva som er viktig, og få problemer med å prioritere riktig.

Evne til å administrere oppgaver

I tillegg til å prioritere må du også kunne administrere de oppgavene du får, på en fornuftig måte. Dette inkluderer både det å planlegge hvordan ulike aktiviteter skal gjennomføres, og å kunne delegere oppgaver til andre. Selv om du ikke har en stilling der du har andre ansatte under deg, vil det fortsatt være oppgaver som bedre kan løses av andre i eller utenfor virksomheten.

Evne til å håndtere stressituasjoner

Uansett hvor godt du planlegger og administrer arbeidsoppgavene, vil det oppstå stressituasjoner. Kritiske systemer bryter gjerne sammen på det verst mulige tidspunkt, og viktige oppgaver har en lei tendens til å hope seg opp. Å kunne holde hodet kaldt, slik at du kan løse oppgavene i tur og orden, er derfor en vesentlig egenskap.

En annen side av dette er evnen til å forholde seg rolig overfor frustrerte eller til og med sinte brukere. Å kunne opptre profesjonelt uansett situasjon er viktig.

Evne til å arbeide selvstendig

Selv om du arbeider sammen med andre i en IT-avdeling eller en helpdesk, er det sjelden at flere deler på de samme arbeidsoppgavene. Evne til å kunne ta avgjørelser og bestemme hva som er viktig når det gjelder de oppgavene du selv er satt til å løse, er derfor viktig. En IKT-medarbeider som sitter med hendene i fanget og venter på å bli fortalt hva han eller hun skal gjøre, blir som regel ikke lenge i jobben.

Det gjelder å holde hodet kaldt..
Fotograf: Corbis

Evne til å tenke systematisk

Brukerstøtte krever at du klarer å håndtere og systematisere mye informasjon og mange detaljer samtidig for å få oversikt over og forståelse for et problem. Effektiv feilsøking krever også at du er i stand til å jobbe systematisk og strukturert.

Evne til å kunne kommunisere godt

En IKT-medarbeider må kunne kommunisere med alle typer brukere på en måte som er forståelig. Medarbeideren må også ta seg tid til å forklare hvorfor et problem oppstod, hvordan det kan unngås i framtida, og hvor og hvordan brukeren kan få mer hjelp uten å føle seg dum.

En annen viktig del av jobben er dokumentasjon og skriftlig kommunikasjon. At du kan ordlegge deg presist skriftlig, er derfor en klar fordel.

Husk alltid å forholde deg til brukerne på en respektfull måte, og bruk tid på å forklare, slik at de forstår.
Fotograf: Corbis

Evne til å løse problemer

Uansett hvor mye du kan om datamaskiner og program, vil det alltid dukke opp nye og ukjente problemer. Den generelle evnen til å løse problemer er derfor en svært nyttig egenskap for en IKT-medarbeider. Dyktige IKT-medarbeidere er som regel også flinke til å løse logiske problemer, forholde seg til store informasjonsmengder og få med seg detaljer.

Tålmodighet

Feilsøking og problemløsing kan være en tålmodighetsprøve i seg selv, men her tenker vi først og fremst på tålmodighet med andre mennesker.

Serviceinnstilling

Brukerstøtte er først og fremst en servicefunksjon. Den viktigste oppgaven er å sørge for at andre får løst arbeidsoppgavene sine uten at problemer med maskinen eller programmene skaper unødige forsinkelser. De fleste brukere er takknemlige når de får hjelp, og en IKT-medarbeider må være bevisst på servicerollen sin.

Som du ser, bør en IKT-medarbeider ha mange egenskaper i tillegg til de IKT-faglige. Men kikker du en gang til på lista, vil du oppdage at disse egenskapene egentlig er ganske vanlige krav for mange typer stillinger og jobber.

Sånn sett er det ikke noe spesielt med IKT-medarbeidere. Poenget er at man ofte overser betydningen av slike egenskaper på bekostning av det IT-faglige, men til sjuende og sist er det selvsagt fagkunnskapen som er avgjørende for å kunne arbeide som IKT-medarbeider.

Uansett hvor teknisk flink du er, er det til liten nytte hvis du ikke er i stand til å bruke kunnskapene dine i en arbeidssituasjon.

Kan det læres?

Et naturlig spørsmål er om man kan lære de generelle egenskapene på samme måte som de IT-tekniske kunnskapene. Svaret er både ja og nei. Egenskapene som er listet opp over, krever ofte øvelse og erfaring og er til en viss grad også knyttet til ens personlighet, men det er fullt mulig å bli bedre. Det viktigste er likevel at du er bevisst på at disse egenskapene er viktige i jobbsituasjonen, slik at du oppdager hvor du har dine egne svakheter, og kan øve deg på å takle de situasjonene som skaper problemer for deg.

Hva forventes av en IKT-medarbeider?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hva forventes av en IKT-medarbeider? (102220)

Som IKT-medarbeider må du regne med å måtte jobbe overtid. Noen oppgaver må nemlig gjøres på tidspunkter da de ikke skaper problemer for andre ansatte.

Det er vel ganske innlysende at en arbeidsgiver i utgangspunktet forventer den samme arbeidsmoralen hos IKT-medarbeidere som hos andre ansatte. Det er naturlig at du kommer på jobben til riktig tid, følger de reglene som gjelder, og ellers oppfører deg ordentlig.

Samtidig forventes det ofte også at du kan være fleksibel når det gjelder arbeidstid. Noen planlagte oppgaver må gjøres på tidspunkter da de skaper minst mulig problemer for andre ansatte. Eller det kan oppstå akutte situasjoner som krever innsats ut over vanlig arbeidstid. Når kritiske systemer ikke fungerer som de skal, og konsekvensene av ikke å få systemene opp igjen kan være store, møter man som regel liten forståelse dersom man går hjem klokka 16.

Ny kunnskap er alltid viktig!

I utgangspunktet forventes det selvsagt at du har IKT-faglige kunnskaper, men det forventes også at du har evne og vilje til å holde deg oppdatert og lære nye systemer. Samtidig er det gjerne slik at ledelsen ikke har noen oversikt over hvilke kunnskaper du vil ha behov for i framtida, så det forventes at du selv gir beskjed om bøker du gjerne vil lese, og kurs du trenger.

Arbeidsklær

La oss si noen få ord om klær også. IKT-medarbeidere er nok ikke først og fremst kjent for sin utpregede stilsans, og mange norske virksomheter har et ganske avslappet forhold til arbeidstøy.

Selv om arbeidsplassen ikke krever at du bruker et bestemt arbeidsantrekk, bør du tenke på at måten du kler deg på, sender et signal til andre om hva slags holdning du har til jobben.

Når kritiske systemer ikke fungerer som de skal, og konsekvensene av ikke å få systemene opp igjen kan være store, møter man som regel liten forståelse for at man går hjem klokka 16.

Fotograf: Berit Roald

Fotograf: Corbis

Du bør derfor være bevisst på hvilke klær du har på deg. Det beste er å venne seg til alltid å være normalt pent kledd på jobben. Da gjør du et bedre inntrykk, og du blir oppfattet som mer seriøs og profesjonell. Du slipper også pinlige situasjoner hvis du for eksempel plutselig må delta i et møte eller lignende, der det hadde vært greit å være skikkelig kledd. Forsøk å finne passende arbeidsantrekk som verken er for uformelle eller for formelle.

Utenfor Norges grenser forventes det ofte at IKT-medarbeidere har et pent og profesjonelt arbeidsantrekk til daglig. Hvis du skal arbeide, delta på kurs, møter eller seminar i utlandet eller møte utenlandske kollegaer og andre som besøker virksomheten du jobber i, bør du derfor være spesielt oppmerksom på hva slags inntrykk du gir.

Urealistiske forventninger til IKT-medarbeidere

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Urealistiske forventninger til IKT-medarbeidere (102226)

Av og til kan du oppleve at virksomheten eller brukerne har urealistiske forventninger til dine evner og til hva du skal gjøre.

Det er særlig på fire områder du kan oppleve urealistiske forventninger:

- kunnskaper (du skal kunne absolutt alt)
- hvor lang tid en oppgave tar
- når og hvor mye du skal jobbe
- hva du skal gjøre

Urealistiske forventninger til kunnskaper

Personer som ikke selv arbeider med IKT-løsninger, har sjelden oversikt over hvor omfattende dette fagfeltet er. Det er et kjent fenomen at jo mer man lærer om datamaskiner, jo mindre føler man at man kan. Det er fordi man stadig oppdager hvor mye mer det er å lære innenfor de enkelte delområdene.

For de fleste er det opplagt at selv om man har gode kunnskaper på ett område, er man ikke nødvendigvis ekspert på alle andre områder som ligner. Har man for eksempel sertifikat for bil, betyr ikke det at man også er kvalifisert til å føre motorsykkel, buss, tog, småfly, seilbåt, paraglider og luftputebåt.

Når det gjelder IKT, vil du imidlertid møte mennesker som tror at siden du jobber med datamaskiner, kan du absolutt alt om det som har med teknologi å gjøre. Denne uklare oppfatningen om hva en IKT-utdannelse kvalifiserer for, gjør at du av og til blir bedt om å påta deg eller blir pålagt arbeidsoppgaver som du ikke har forutsetninger for å kunne klare.

Selv om du skal være serviceinnstilt og selvsagt ikke bør takke nei til enhver utfordring, må du også kjenne din begrensning. Du bør ikke si ja til oppgaver du vet du ikke kan løse.

Når du sier nei til en oppgave, er det viktig at du også forklarer hvorfor du ikke kan eller bør gjøre den. Hvis du bare sier at du ikke kan det du blir bedt om, uten å forklare at dette er noe som ligger utenfor ditt arbeidsfelt, kan vedkommende som spør, enten tro at du er lite samarbeidsvillig, eller at du ikke kan faget ditt.

Urealistiske forventninger til hvor lang tid en oppgave tar

Ting tar tid, og det som kan se ut som en forholdsvis enkel oppgave, kan fort vise seg å bli et problem som det tar timer eller dager å løse. Du må akseptere at brukere av og til tror at et problem er lett å fikse, og forsøke å forklare hvorfor løsningen er mer komplisert og tar lengre tid.

De fleste urealistiske forventninger til hvor lang tid det vil ta å gjøre en jobb, er det imidlertid IKT-medarbeideren selv som er skyld i. Hvis du ikke tar hensyn til at det kan dukke opp uforutsette problemer (noe det svært ofte gjør), og gir et tidsestimat basert på hvor lang tid det vil ta å gjøre jobben under ideelle forhold, skal det ikke mye til før tidsskjemaet sprekker. Ikke så å forstå at du konsekvent skal si at alt tar mye lengre tid enn det faktisk gjør, men du bør alltid legge inn en sikkerhetsmargin. Husk også at jo mer komplisert en oppgave eller et system er, jo flere uforutsette problemer vil du kunne støte på.

Urealistiske forventninger til når og hvor mye du skal jobbe

Du kan oppleve at andre ansatte har liten forståelse for at du som IKT-medarbeider også har en arbeidstid, og at du, selv om du er interessert i data, ikke har lyst til å bruke all din våkne tid på jobben.

- Et vanlig «krav» du kan risikere å møte, er at du skal ordne et problem i lunsjen, slik at brukeren ikke blir forstyrret i arbeidet sitt. Brukeren tenker ikke på at du også har behov for lunsjpause.
- Et annet «krav» kan være at du skal ordne et problem etter arbeidstid – eller i helgen – slik at alt er i orden når brukeren kommer på jobb neste morgen. Begrunnelsen for dette er gjerne at jobben vedkommende holder på med, er så viktig at det *må* være i orden neste morgen. Av og til er dette selvsagt riktig, og i så fall må du akseptere at det blir overtid den kvelden, men det er slett ikke alltid det stemmer. Her ser vi igjen at god kunnskap om bedriften er vesentlig for å kunne ta en kvalifisert avgjørelse. Legg merke til at hvis du løser problemet om kvelden, er det du som må jobbe overtid. Hvis du løser problemet neste formiddag, er det kanskje brukeren som må jobbe overtid.

Vi må nok en gang understreke at avsnittene over ikke må oppfattes dit hen at man konsekvent skal si nei til all jobbing ut over vanlig arbeidstid. Som vi har sett tidligere, er det ikke uvanlig at IKT-medarbeidere må stille på jobb til ukurante tider, og av og til vil konsekvensene av å si nei kunne bli store for virksomheten. Du må derfor kunne skille mellom det som er viktig, og det som er urimelig.

Urealistiske forventninger til hva du skal gjøre

Det er ikke alltid alle har en like klar oppfatning av hva som er en IKT-medarbeiders oppgaver. Det skjer derfor at noen forventer at du skal løse problemer eller gjøre oppgaver som ligger langt utenfor det stillingen egentlig innebærer.

Det er for eksempel vanlig å få forespørsel om å fikse kopimaskiner, telefoner, mobiltelefoner, kontormøbler, arbeidslamper og så videre. Før du sier ja til slike forespørsler, bør du stille deg selv følgende tre spørsmål: Er dette noe jeg kan? Kan jeg gjøre dette uten at det går ut over andre oppgaver jeg skulle ha gjort? Er det dette virksomheten betaler meg for? Hvis svaret på ett av disse spørsmålene er nei, bør du svare pent nei til henvendelsen.

En annen ting du bør passe deg for, er brukere som forventer at du skal gjøre jobben for dem. Det finnes mange varianter og nyanser her, men det er for eksempel stor forskjell på det å løse et problem i et regneark og det å lage hele regnearkmodellen.

Klarer med en overordnet dersom du blir bedt om å reparere en ansatts private laptop.
Fotograf: Corbis

Du kan også risikere å oppleve at noen tar med seg sin private hjemmemaskin på jobben og regner med at du skal fikse den gratis. Noen kan også forvente at du skal komme hjem til dem etter arbeidstid og løse dataproblemer for dem der.

Det er selvsagt ikke noe i veien for å være hyggelig, men du bør være svært forsiktig med å svare ja til for mange slike forespørsler. Slike «enkle» problemer tar gjerne betydelig mer tid enn du blir forespeilet, og har du først sagt ja til å løse ett problem, blir det vanskeligere å si nei neste gang du blir spurt.

Virksomheten betaler deg ikke for å fikse de ansattes private datamaskiner, så det er viktig å få godkjent denne typen oppdrag først hvis jobben skal gjøres i arbeidstida. Hvis virksomheten er villig til å betale deg for å bruke av arbeidstida til å reparere de ansattes private datamaskiner, er det greit nok, men i de fleste tilfeller vil ikke virksomheten være spesielt interessert i dette.

Du kan oppleve at virksomheten eller brukerne har urealistiske forventninger til dine evner og hva du skal gjøre.

Møte med brukerne

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Møte med brukerne (102248)

Brukerstøtte handler like mye om mennesker som om teknologi. Som IKT-medarbeider må du aldri glemme at det er du som er der for dem, og ikke omvendt.

Selv om jobben din er å sørge for at maskiner og program fungerer som de skal, må du hele tida forholde deg til dem som er avhengige av IKT-systemene for å få gjort jobben sin. En dyktig IKT-medarbeider passer ikke bare på at maskiner og program fungerer som de skal, men sørger også for at brukerne får utnyttet systemene på best mulig måte.

Opptre respektfullt overfor alle brukere. Unngå ord og uttrykk som får brukeren til å føle seg dum.
Fotograf: Corbis

I møte med brukerne er det tre regler du må huske. Vi kan godt kalle dem IKT-medarbeiderens gylne regler:

1. Opptre aldri nedlatende overfor brukeren.
2. Aldri si eller gjør noe som får brukeren til å føle seg dum.
3. Ikke kritiser eller kjeft på brukeren.

Opptre aldri nedlatende overfor brukeren

At man ikke skal oppføre seg nedlatende overfor andre, er en del av vanlig folkeskikk og burde vel være en selvfølge også når det gjelder brukerstøtte. Men av og til kan man virke nedlatende eller arrogant uten at man egentlig har ment det slik.

Et eksempel er hvis man bagatelliserer brukerens problemer, arbeidsoppgaver eller betydningen av disse. Selv om du kanskje har ting å gjøre som haster mer, eller vet at den oppgaven som brukeren forsøker å løse, ikke er så viktig, har brukeren fortsatt krav på respekt.

Hvis du ikke kan hjelpe en bruker med en gang fordi det er andre oppgaver som haster mer, så ikke opptre på en slik måte at brukeren får følelsen av ikke å være viktig. Husk at det som kan virke som en bagatell for deg, kan ha stor betydning for brukeren.

Aldri si eller gjør noe som får brukeren til å føle seg dum

Det er fort gjort å være litt ubetenksom når man skal forklare hva som er årsaken til en feil eller et problem. En del av de problemene du løser som IKT-medarbeider, skyldes brukerfeil, at brukeren forsøker å gjøre noe som er umulig, eller rett og slett ikke forstår hvordan noe skal gjøres.

For å si det enkelt – brukere gjør av og til dumme ting. Men ingen liker å bli kalt dum, verken direkte eller indirekte, og hvis brukeren faktisk har gjort noe dumt, vet vedkommende det som regel selv. Vær diplomatisk, og velg dine ord med omhu når du forklarer en bruker som har gjort noe dumt, hva som har gått galt.

Ikke kritiser eller kjeft på brukeren

Det kan være vanskelig å beholde roen hvis brukeren stiller urealistiske krav, begynner å kritisere eller til og med hisser seg opp fordi maskinen ikke fungerer og du ikke klarer å fikse den der og da.

Brukere er en variert gruppe mennesker. Enkelte tror at de får bedre og raskere hjelp hvis de oppfører seg som bøller. Du skal selvsagt ikke finne deg i all slags oppførsel fra brukerne, men i utgangspunktet skal du alltid opptre profesjonelt og la brukeren få gi uttrykk for eventuell frustrasjon.

Det er dessverre slik at IKT-medarbeideren av og til blir offer for brukernes frustrasjon over datamaskinen. Det er ikke så lett å kjefte på en datamaskin, og frustrasjonen kan ha bygd seg opp i lang tid før du kommer for å se på problemet. Vedkommende kan for eksempel ha mistet data og må gjøre mye arbeid om igjen.

Hvis du begynner å kritisere eller kjefte på brukeren i en slik situasjon, blir vedkommende bare ytterligere opphisset. Prøv i stedet å se det fra brukerens side, og forsøk å opptre støttende.

Husk at frustrasjonen hos brukeren kan ha bygd seg opp en god stund før du som IKT-servicemedarbeider blir kontaktet.
Fotograf: Matthias Tunger

Brukerstøtte handler like mye om mennesker som om teknologi.

Kommunisere med brukere

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kommunisere med brukere (102249)

Det er to ting som er vesentlige når du snakker med brukerne. Du må ta deg tid til å lytte, og du må være sikker på at du blir forstått.

Det er lett å glemme at ord og begreper som det er naturlig for deg å benytte i IKT-sammenheng, ikke alltid blir forstått av dem som ikke jobber med IKT til daglig. Innholdet i et begrep kan være opplagt for deg, men uklart for brukeren.

Det er for eksempel ikke uvanlig å tro at harddisken er det samme som hele datamaskinen. Så hvis du sier at harddisken må skiftes, tror brukeren kanskje at han eller hun skal få en ny datamaskin.

En dyktig IKT-medarbeider tar seg alltid tid til å forklare hva som er feilen, og hva man har gjort for å rette den, men du må tilpasse forklaringen til det kunnskapsnivået brukeren har.

Det at vedkommende nikker og sier ja mens du forklarer, er ingen garanti for at han eller hun faktisk forstår hva du sier. Mennesker er generelt lite flinke til å si fra når det er noe de ikke forstår, spesielt hvis de tror at det er noe de burde ha forstått, eller hvis de føler at det å spørre kan få dem til å virke dumme.

I tillegg til å uttrykke deg klart må du også ta deg tid til å lytte til hva brukerne sier. Det er brukerne som opplever problemet, og som best kan beskrive hva det består i.

En annen ting er at det oppfattes som uhøflig å avbryte andre som snakker, eller å overse det de sier. Du bør derfor la brukeren få lov til å forklare seg selv om du vet hva problemet er. Det hender også at du må bruke litt ekstra tid for å la brukeren få lov til å snakke om ting som opptar vedkommende, eller rett og slett bare få lufte sine frustrasjoner over datamaskinen.

Ta deg alltid god tid til å forklare hva brukeren eventuelt har gjort feil ved bruk av pc-en.
Fotograf: Nicolai Howalt

Det er to ting som er vesentlige når du snakker med brukerne. Du må ta deg tid til å lytte, og du må være sikker på at du blir forstått.

Brukernes kunnskapsnivå

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Brukernes kunnskapsnivå (102251)

Brukere er forskjellige og har varierende grad av IKT-kunnskap. Noen har minimale kunnskaper og forstår kanskje ikke engang grunnleggende datauttrykk. Andre har mange års erfaring og kan være eksperter på noen områder. Som IKT-medarbeider må du kunne forholde deg til brukere med ulikt kunnskapsnivå.

Brukernes kunnskapsnivå kan grovt deles inn i tre:

- liten eller ingen kunnskap
- normal kunnskap
- mye kunnskap

Lavt kunnskapsnivå

Det kan være flere grunner til at noen kan lite eller ingenting om hvordan de skal bruke en datamaskin. Kanskje har de ganske enkelt ikke hatt behov for eller mulighet til å skaffe seg mer datakunnskap tidligere. De har kanskje ikke brukt en datamaskin i jobben før og ikke følt noe behov for å ha en hjemme. Det kan godt være at brukere har vært på kurs, men at de av en eller annen grunn har fått lite utbytte av det.

Brukere med et lavt kunnskapsnivå har ofte problemer som er enkle å løse, men som likevel tar mye tid, og du kan fort ende opp med å gjøre brukerens jobb. En oppgave for IKT-medarbeideren er derfor å hjelpe brukeren opp på et normalt kunnskapsnivå. Brukeren er som regel klar over sin egen situasjon og er takknemlig for den hjelpen du kan gi. Ofte føler vedkommende også at det er litt flaut å måtte spørre så mye om helt enkle ting, og vil derfor gjerne lære å klare seg selv.

Jobbsituasjonen til en IKT-medarbeider tillater sjelden at man kan bruke tida til spesialopplæring for en enkelt bruker, men virksomheten er som regel positivt innstilt til at det arrangeres interne kurs for flere ansatte. Halvdagskurs for tre–seks brukere, der du fokuserer på noen bestemte tema som du vet at disse brukerne sliter med, er ofte en svært god investering både for deg og for virksomheten.

Et annet mulig tiltak er å skaffe brukeren en god lærebok eller et opplæringsprogram som vedkommende kan studere på egen hånd.

Normalt kunnskapsnivå

De fleste brukere har det vi kan kalle et normalt kunnskapsnivå. Det vil si at de er i stand til å bruke maskinen til vanlige arbeidsoppgaver og finne ut av enkle problemer på egen hånd. De gjør som regel heller ikke så mange alvorlige feil. Selv om «vanlige» brukere ofte klarer seg greit, må du ikke glemme at også disse har behov for opplæring og oppfølging. Spesielt gjelder det når det skjer endringer, som for eksempel programoppgraderinger.

Høyt kunnskapsnivå

De fleste har i dag én eller flere datamaskiner hjemme, og mange er også interessert i data som hobby. Mange bedrifter har derfor brukere med et relativt høyt kunnskapsnivå.

Brukere med et høyt kunnskapsnivå har normalt få problemer selv og får ofte status som «lokal dataguru» i den avdelingen de jobber. Andre brukere spør gjerne slike personer om hjelp før de tar kontakt med brukerstøtte.

Brukere med høyt kunnskapsnivå fungerer derfor i mange sammenhenger som en avlastning for IKT-support, men du skal være forsiktig med å oppmuntre for mye til slik virksomhet. Selv om mange trives med statusen som «dataguru» blant kollegaene, bør du aldri be andre ansatte om å spørre vedkommende om hjelp før de tar kontakt med brukerstøtte. For det første er det slett ikke sikkert at brukeren i lengden er så fornøyd med å gjøre jobben din på bekostning av sin egen. Det er heller ikke sikkert at avdelingslederen eller ledelsen i bedriften er særlig fornøyd med at du skyver jobben din over på andre ansatte.

Et annet mulig problem er at enkelte later som om de forstår eller kan mer enn hva som egentlig er tilfellet, og dermed gir seg i kast med å løse problemer de ikke har forutsetninger for å håndtere. Da kan man fort ende opp med et problem som er atskillig mer komplisert og tidkrevende når man overtar, enn det var i utgangspunktet.

Brukere med et høyt kunnskapsnivå er som sagt gjerne selvhjulpne, men ofte også mer krevende når de først får problemer. De bruker gjerne flere program og flere avanserte funksjoner enn gjennomsnittsbrukeren, og når det først oppstår et problem, er dette derfor gjerne ukjent.

Enkelte ansatte har bakgrunn fra yrker der de har benyttet andre verktøy enn pc i sitt daglige arbeid. Som IKT-servicemedarbeider bør du utvise tålmodighet og forståelse, slik at den ansatte raskt lærer å beherske pc-en.
Fotograf: Olav Olsen

Superbrukere

En egen kategori av brukere med høyt kunnskapsnivå er dem vi kan kalle «superbrukere». Dette er brukere som kan svært mye om et spesielt system eller program. Slike brukere kan være svært verdifulle for deg som IKT-medarbeider, spesielt hvis de har kompetanse på program eller systemer som du ikke kjenner godt selv.

De fleste virksomheter har systemer som er knyttet til et bestemt fagområde eller en spesiell del av virksomheten. En bruker som arbeider med et slikt system til daglig, og som kanskje også har vært involvert i utviklingen av det, vil ha en kompetanse som du vanligvis ikke har mulighet til å skaffe deg selv. Kunnskap om slike systemer er ofte knyttet til det fagområdet de benyttes på, slik at du også må forstå fagterminologien og annet som er spesielt for dette faget, for å forstå systemet fullt ut.

Du vil av og til ha behov for den kunnskapen superbrukere sitter med, så det er viktig å ha et godt forhold til disse menneskene og kunne samarbeide med dem. De fleste mennesker har yrkesstolthet og vil gjerne ha anerkjennelse for de fagområdene de behersker godt. Dette bør du være bevisst på når du er i kontakt med superbrukere:

- **Gi uttrykk for at du respekterer brukerens kompetanse** Innse at det er brukeren som kan mest om det aktuelle programmet eller systemet, og hør på hva han eller hun har å si. Ikke se på brukeren som en slags konkurrent som forsøker å overta ditt fagfelt.
- **Gi uttrykk for at du anerkjenner brukerens kompetanse** Gi klart uttrykk for at det er brukeren som kan mest på sitt område, og unngå uttalelser eller handlinger som gir inntrykk av at du bagatelliserer den kompetansen brukeren har. Ved å gi brukeren anerkjennelse for den kompetansen han eller hun faktisk har på det aktuelle området, vil vedkommende være langt mer villig til å bruke av sin tid for å hjelpe deg med å løse eventuelle problemer med det aktuelle systemet i framtida.

På sykehus benyttes en rekke spesialiserte dataprogram. Som IKT-servicemedarbeider vil du måtte samarbeide nært med superbrukerne av slike systemer.
Fotograf: Helen King

Datavegring

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datavegring (102252)

En gruppe brukere som du bør være spesielt oppmerksom på, er den gruppen som har en eller annen form for «datavegring».

«Datavegring» er en betegnelse på skepsis eller negativ innstilling til å bruke datamaskiner. Selv om de fleste nå har akseptert at datamaskiner er et nødvendig og nyttig verktøy, finnes det fortsatt en del som ikke finner seg til rette med å ha en datamaskin foran seg. Det kan være flere grunner til at man er redd for eller misliker datamaskiner:

- Man er generelt skeptisk til teknologi.
- Man føler at datamaskinen styrer jobben.
- Man er redd for å gjøre feil.
- Maskinen får en til å føle seg dum.
- Man likte bedre jobben slik den var før man måtte bruke datamaskin.

Datavegring er et reelt problem som ofte gjør at personen mistrives på jobben. Dette skal du ta på alvor, og som IKT-medarbeider kan du gjøre mye for å hjelpe personer som har utviklet en negativ holdning til IKT.

Fotograf: Steve H. McDonough

Personer med datavegring viser som regel dette på én av to måter. Den ene måten er å være overdrevent negativ og noen ganger nesten fiendtlig innstilt til datamaskiner. Dette gir seg gjerne utslag i negative kommentarer om maskiner og program. Selv små feil og problemer fører gjerne til kommentarer av typen: «Den fordømte maskinen fungerer aldri som den skal.» «Nå må jeg gjøre hele jobben på nytt.» «Det fungerte mye bedre før vi fikk de maskinene.»

Den andre reaksjonsformen er å nedvurdere seg selv i forhold til maskinen. Personen oppfatter seg selv som dum og påtar seg skylden for alt som går galt. «Jeg er for dum til å skjønne hvordan disse maskinene fungerer.» «Jeg klarer aldri å lære dette.» «Nå har jeg sikkert gjort noe galt igjen.»

Alle brukere kan fra tid til annen bli frustrert over dataproblemer. Det som skille personer med datavegring fra andre brukere, er at de alltid er negative overfor maskinen og gjerne gir uttrykk for dette til omverdenen i en overdreven form.

Generell skepsis til teknologi

Noen mennesker føler seg ikke komfortable med teknologi generelt. De kan ha dårlige erfaringer eller føle at teknologien er blitt for dominerende i dagliglivet. Media bidrar også til å fyre opp under en slik skepsis med sine mange oppslag om datavirus, piratkopiering, barnepornografi, spam (søppelpost), svindel og så videre. Personer som i utgangspunktet er skeptiske til teknologien, ser gjerne dette som en bekreftelse på at de har rett.

Datamaskinen styrer jobben

Når man ikke føler at man behersker teknologien, risikerer man å bli fremmedgjort overfor sin egen jobb – man kjenner ikke igjen sin egen jobb slik den var. Arbeidsoppgaver man tidligere hadde full kontroll over, er nå styrt av en datamaskin, og man føler ikke lenger at man har oversikt over hva som skjer. Videre er det ikke uvanlig at man føler seg nedvurdert i forhold til maskinen fordi det er den og ikke en selv som gjør jobben, og dermed også utrygg når det gjelder egen jobbsikkerhet.

Man er redd for å gjøre feil

Enkelte brukere er nesten livredde for å gjøre feil. Alle mennesker har en trygghetssone når det gjelder hva man føler at man behersker, og når man beveger seg på utsiden av denne sonen, føler man seg usikker og blir redd for å gjøre selv små feil. Når det gjelder datamaskiner, gir dette seg ofte utslag i at de lærer seg nøyaktig hva de må gjøre for å få utført en bestemt oppgave. Ofte følger de rene oppskrifter og har ingen egentlig forståelse for eller kunnskap om hva de faktisk gjør. De vet bare hva som blir resultatet når de følger oppskriften. Slike brukere stopper opp så fort det skjer noe uventet. Typisk vil de heller starte maskinen på nytt og begynne fra begynnelsen enn å forsøke å løse et problem som oppstår.

Man føler seg dum i forhold til maskinen

Ikke alle mennesker har like mye selvtillit, og hvis man ikke kan noe særlig om datamaskiner, er det fort gjort å oppfatte maskinen som smartere enn en selv. Noen brukere tillegger datamaskiner egenskaper som de ikke har i virkeligheten. Kombinert med et dårlig selvbilde kan dette resultere i datavegring. Man føler seg rett og slett dum i forhold til maskinen.

Man likte jobben sin bedre før

Endringer i arbeidssituasjon er noe nesten alle opplever. Noen ganger er innføringen av datasystemer årsaken til endringene, men ofte blir datamaskinen gjort til syndebukk for endringer som ville kommet uansett. Det vil alltid være mennesker som synes at «alt var så mye bedre før, da man ikke hadde datamaskiner».

Selv om vi her har delt inn årsakene til datavegring i enkle kategorier, kan årsakene ofte være sammensatte. For eksempel vil en person som er redd for å bruke en datamaskin, ofte også føle seg dum i forhold til den og ganske sikkert synes at jobben var bedre før.

Datavegring kan være et stort problem, og det er ingen enkle eller raske måter å endre en persons holdninger på. Som IKT-medarbeider skal du heller ikke fungere som «psykolog» for slike brukere, men du bør selvsagt forsøke å hjelpe dem så langt det er mulig.

La brukeren få lov til å forklare problemene, og forsøk å komme med forslag til hva som kan gjøres for å forbedre situasjonen. Bruk tid på å forklare hvordan ting faktisk fungerer, og forsøk å få brukeren til å se noen av fordelene datamaskiner kan ha. Brukere som er redde for å gjøre feil, bør oppmuntres til å forsøke allikevel.

Ofte er det eldre arbeidstakere som lider av datavegring. Mange av dem har ikke fått god nok opplæring i hvordan de skal bruke de ulike typene programvare.
Fotograf: NTB scanpix

Personer som lider av datavegring, er ofte overdrevent negative til datamaskiner eller nedvurderer seg selv i forhold til maskinen.

Feilsøkingsmetodikk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Feilsøkingsmetodikk (102254)

Som IKT-medarbeider vil du bli bedt om å løse problemer som du ikke har noen erfaring med fra før. Da er det nødvendig med en systematisk framgangsmåte.

Systematisk feilsøking og problemløsing kan oppsummeres i sju punkter:

1. Kartlegge omstendighetene rundt feilen
2. Reprodusere feilen
3. Lokalisere og begrense feilkildene
4. Innhente nødvendig informasjon
5. Bestemme mulige løsninger
6. Teste ut mulige løsninger
7. Dokumentere feilen og løsningen

1. Kartlegge omstendighetene rundt feilen

Det første du må gjøre, er å kartlegge omstendighetene rundt feilen. Dette gjøres ved å spørre brukeren om feilen. Under følger en liste over de mest aktuelle spørsmålene. Merk at alle spørsmålene ikke nødvendigvis er like relevante for alle typer problemer, og at rekkefølgen det er naturlig å stille spørsmålene i, vil variere.

Hva består problemet i? Be brukeren om å beskrive hva feilen består i. Dette hjelper deg til å fastslå hva det er brukeren forsøker å gjøre. Hvis det er snakk om et brukerproblem, kan du ofte allerede her fastslå hva som er problemet, og løse det. Men hvis feilen er relatert til maskin eller programvare, er det at brukeren ikke klarer å få gjort det han eller hun ønsker, bare et symptom på den faktiske feilen.

Når oppstod feilen? Det hender at brukere har hatt et problem i lengre tid, men ikke brydd seg om å melde fra. De har funnet en annen måte å få gjort tingene på, eller feilen har ikke vært så stor at det har skapt vesentlige problemer i jobben deres.

Hvem brukte datamaskinen da feilen oppstod eller ble oppdaget? Hvis det er flere som bruker samme maskin, eller du er usikker på om du snakker med den som oppdaget feilen, er det greit å få fastslått hvem som var brukeren.

Har denne feilen oppstått tidligere? Mange feil kan være sporadiske. Det vil si at de bare opptrer av og til eller i bestemte situasjoner. Det kan også tenkes at det er en svakhet i systemet som ikke har vært utbedret skikkelig tidligere. Hvis feilen har vært fikset tidligere, er det naturlig å spørre hvem som da løste den, slik at du eventuelt kan ta kontakt med vedkommende for å få vite hva som ble gjort. Hvis bedriften har en rutine for registrering og dokumentasjon av brukerstøtte, bør det også finnes et dokument som redegjør for hva som er gjort tidligere.

Er det andre som har brukt maskinen nylig? Hvis andre har brukt maskinen, kan de ha endret konfigurasjoner, installert programvare, koblet til maskinvare midlertidig eller gjort noe annet som har ført til at maskinoppsettet er endret.

I mars 2012 ble Skatteetatens Altinn-sider brått stengt da det ble oppdaget at man kunne få tilgang til ukjentes personopplysninger. I slike tilfeller haster det med å kartlegge og rette opp feilen.
Fotograf: Espen Sjølingstad Hoen

Er det andre som har eller har hatt det samme problemet? Hvis andre har brukt den samme maskinen, er det naturlig å undersøke om de har opplevd det samme problemet. Det kan også tenkes at det er andre som har eller har hatt det samme problemet på sine maskiner.

Er det blitt installert noen nye program eller oppgraderinger på maskinen nylig?

Er det blitt installert eller skiftet noe deler i maskinen nylig? Det er viktig å fastslå om det er gjort program- eller maskinendringer i forkant av at feilen oppstod. Enhver slik endring er en potensiell feilkilde og et godt utgangspunkt for videre feilsøking.

En mulig feilkilde kan være virusangrep.
Fotograf: Science Photo Library

Er det blitt kjørt noen oppryddingsprogram eller lignende nylig? For eksempel diskdefragmentering, program som rydder opp i *registry*, eller lignende.

Har brukeren slettet noen filer eller manuelt ryddet på maskinen nylig? Det kan tenkes at brukeren ved et uhell har slettet eller flyttet kritiske filer eller mapper.

Har noen andre forsøkt å rette feilen? Hvis feilen har vært forsøkt rettet, for eksempel av brukeren eller andre, kan det opprinnelige maskinoppsettet være endret. Dette er det viktig å være oppmerksom på når du starter feilsøkingen, da tidligere forsøk på å rette en feil kan ha medført at maskinen ikke lenger har den samme konfigurasjonen som da den sist fungerte som den skulle.

Hva tror brukeren er årsaken til feilen? Av og til har brukeren selv en oppfatning om hva som har forårsaket en feil, eller hva som er årsaken til et problem. Brukere med mye IKT-kunnskap vet ofte også hva som er feilen, men mangler det nødvendige utstyret eller rettighetene til å kunne fikse den selv.

Spørsmålene over vil ofte være nok til at du kan fastslå hva som er galt, og rette feilen. Hvis ikke har du i hvert fall kartlagt omstendighetene rundt feilen og kan ta fatt på selve feilsøkingen.

2. Reprodusere feilen

Når du har kartlagt omstendighetene rundt en feil, er det neste steget å forsøke å reprodusere den. Det er ikke alltid det er behov for å reprodusere en feil. Vi skiller mellom permanente, konsekvente og sporadiske feil.

En svart skjerm kan være et eksempel på en såkalt permanent feil.
Fotograf: Science Photo Library

En **permanent feil** er en feil som opptrer hele tida. At en maskin ikke får kontakt med nettet, en svart skjerm eller at maskinen ikke starter, er eksempler på permanente feil.

En **konsekvent feil** er en feil som alltid oppstår som resultat av en bestemt handling eller en serie handlinger. Når et program henger seg hver gang man forsøker å bruke en bestemt funksjon, er det snakk om en konsekvent feil.

Sporadiske feil er feil som opptrer av og til, men ikke som følge av en bestemt handling eller i en bestemt situasjon. Typisk vil det at program plutselig avsluttes uten noe forvarsel, eller at maskinen slår seg av tilfeldig, være eksempler på sporadiske feil.

Det er særlig når det gjelder sporadiske feil, at du bør forsøke å finne en måte å reprodusere feilen på. Som hovedregel er det enklere å feilsøke permanente feil enn konsekvente og enklere å feilsøke konsekvente feil enn sporadiske. Hvis du kan reprodusere en sporadisk feil, slik at den opptrer konsekvent, vil det som regel gjøre den videre feilsøkingen enklere.

For å reprodusere en feil bør du la brukeren forklare hva vedkommende gjorde da feilen oppstod, og gjenta dette steg for steg. Forsøk å få med alle detaljer – som hvilke andre program som kjørte samtidig, om det var startet noen eksterne jobber (for eksempel søk i en database), utskriftsjobber eller annet som kan ha hatt betydning.

3. Lokalisere og begrense feilkildene

Når du har et klart bilde av hva problemet består i, og i hvilke sammenhenger det opptrer, er neste steg å begrense de mulige feilkildene. Noen ganger er årsaken opplagt, men i mange tilfeller er det flere mulige årsaker til en feil. En svart skjerm kan for eksempel skyldes feil med skjermen, feil på strømforsyningen til skjermen, feil på kabelen mellom skjermen og maskinen, feil på skjermkortet, dårlig kontakt mellom skjermkortet og hovedkortet, feil driver for skjermkortet, feil innstilling av skjermen (lysstyrke og kontrast), feil konfigurasjon av skjermoppløsningen i operativsystemet eller feil konfigurasjon av multiskjermfunksjonen i operativsystemet.

Når du starter denne delen av feilsøkingen, bør du derfor begynne så bredt som mulig og forsøke å eliminere de faktorene som ikke kan være årsak til feilen.

Det er naturlig å begynne med å forsøke å avgjøre om feilen skyldes maskinvare eller programvare. Deretter jobber du deg systematisk videre til du har begrenset feilkildene så mye som mulig.

Hensikten med å begrense feilkildene er å begrense de mulige løsningene du trenger å innhente informasjon om og teste ut. Hvis du kan isolere problemet til en bestemt enhet (nettverkskort, skriver, skjerm og så videre) eller et bestemt program, forenkler det arbeidet med å innhente informasjon om mulige løsninger.

Utrangerte datakort til PC.

Fotograf: Svein Grønvold

4. Innhente nødvendig informasjon

Før du fortsetter feilsøkingen, bør du undersøke om det allerede finnes informasjon om det problemet du forsøker å løse. Mange feil er kjent og løsningene dokumentert av produsenten. Hvis du har klart å isolere problemet til en bestemt enhet eller et bestemt program, er det naturlig enten å ta kontakt med leverandørens supporttjeneste eller forsøke å finne informasjon om det aktuelle problemet i håndboka eller på leverandørens nettsider

Mange store IKT-leverandører har gode hjemmesider med informasjon om løsninger på vanlige problemer.

Opphavsmann: Intel

5. Bestemme mulige løsninger

Når du har begrenset de mulige feilkildene og innhentet den informasjonen som er tilgjengelig om utstyret og den aktuelle feilen, kan du avgjøre hvilke mulige løsninger som bør testes ut. Hvis feilen er svært komplisert, kan det være nødvendig først å systematisere mulighetene ved å skrive dem opp og ordne dem i den rekkefølgen de bør forsøkes, slik at du prøver de mest sannsynlige løsningene først. Det kan også være nødvendig å prøve ut ulike løsninger i en bestemt rekkefølge.

6. Teste ut mulige løsninger

Når det er klart hvilke muligheter du bør forsøke, må disse testes ut. I en feilsøkingsprosess er det viktig at du arbeider deg gjennom de ulike alternative løsningene i tur og orden og aldri gjør mer enn én endring av gangen. Hvis mulig bør du også reversere én endring før du forsøker den neste, slik at du alltid starter fra det samme utgangspunktet.

Hvis du gjør flere endringer samtidig, mister du lett oversikten over hva som eventuelt løser feilen, og det blir vanskeligere å fastslå hva som faktisk var årsaken. En endring du gjør i forbindelse med feilsøking, kan av og til også forårsake nye problemer eller feil, og med flere samtidige endringer kan det være vanskelig å si hva som skapte det nye problemet.

7. Dokumentere feilen og løsningen

Siste ledd i feilsøkingsprosessen er å dokumentere feilen og løsningen på problemet. Det gjelder også de gangene du ikke finner en løsning. Noen ganger vil den raskeste og rimeligste løsningen være å skifte ut en maskin eller reinstallere programvaren. I så fall bør feilen og de løsningene du har forsøkt, dokumenteres, slik at du har et grunnlag å arbeide ut fra hvis problemet oppstår igjen.

Også i de tilfellene der feilen løses, må du selvsagt dokumentere hva som var årsaken til feilen, og hvordan den ble løst. Slik dokumentasjon er vesentlig både med tanke på framtidig feilsøking og når man skal føre statistikk over antall og typer feil.

Driftsstøtte

Organisering av driftsstøtte

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Organisering av driftsstøtte (102304)

Den beste formen for brukerstøtte er å forhindre at brukerne i utgangspunktet får problemer. Selv om du ikke har noen garanti mot at brukere gjør feil, eller at det oppstår feil på maskiner eller programvare, kan du gjøre mye for å forebygge problemer.

Driftsstøtte handler om drift og vedlikehold av en virksomhets IKT-infrastruktur, det vil si maskiner, servere, nettverk, programvare, data og tilganger.

Ved å sørge for at IKT-infrastrukturen er oppdatert og fungerer som den skal, bidrar du til at brukerne opplever færre problemer, og behovet for brukerstøtte blir mindre.

Mange av oppgavene som er knyttet til driftsstøtte, skal utføres regelmessig og bør derfor organiseres som faste rutiner, slik at du kan være sikker på at de blir utført som planlagt, og kan kontrollere at de blir gjort riktig.

Spesielt er gode rutiner for **sikkerhetskopiering** viktig. Det bør også finnes egne planer for vedlikehold og oppdateringer.

Store bedrifter – som her CERN i Sveits – stiller strenge krav til drift og vedlikehold av servere og IKT-infrastruktur.
Fotograf: Vincent Moncorgé

Driftsstøtte handler om drift og vedlikehold av en virksomhets IKT-infrastruktur.

Sikkerhetskopiering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikkerhetskopiering (102306)

Alle virksomheter må ha en rutine for sikkerhetskopiering, men det slurves dessverre mye.

Det er ikke nok bare å kjøre regelmessig sikkerhetskopiering. Det må finnes en rutine som sikrer at kopieringen utføres riktig, at kopiene oppbevares trygt, og at det er mulig å legge kopien tilbake hvis man mister data.

En god rutine for sikkerhetskopiering bør inneholde informasjon om

- hvor ofte det skal kjøres sikkerhetskopiering
- når det skal kjøres sikkerhetskopiering
- hva slags sikkerhetskopiering som skal utføres
- hva det skal tas kopi av
- hvem som er ansvarlig for at det kjøres sikkerhetskopiering
- hvem som overtar hvis den ansvarlige ikke er tilgjengelig
- hvordan sikkerhetskopieringen utføres
- hvordan det skal kontrolleres at sikkerhetskopieringen er i orden
- hvor og hvordan sikkerhetskopier skal oppbevares
- hvordan en eventuell tilbakekopiering utføres
- hvem som er ansvarlig for å oppdatere rutinen og kontrollere at den blir fulgt

Du synes kanskje at denne rutinen virker omfattende, men alle punktene er viktige. Det er for eksempel ikke uvanlig at en virksomhet tror de har sikkerhetskopier, men når uhellet er ute og data skal hentes tilbake, viser det seg at kopien er ubrukelig. Man har startet sikkerhetskopieringen hver dag, men ikke oppdaget at den ikke kjørte som den skulle, fordi det ikke var noen rutine for å kontrollere kopien *etter* kjøring.

Alle punkter i rutinen må testes, slik at man er sikker på at de fungerer slik de er ment. Dette er særlig kritisk i forbindelse med **tilbakekopiering** av data. Mange virksomheter har aldri testet om tilbakekopiering fungerer slik det skal, og vet ikke om det virker eller hvor lang tid det tar, fordi de ikke har opplevd en systemkrasj ennå.

Et annet typisk eksempel er utskifting av lagringsmediet som benyttes til sikkerhetskopiering. Etter hvert som datamengdene øker og teknologien utvikler seg, må også metoden og lagringsmedia for sikkerhetskopier oppgraderes.

En felle mange har gått i, er at de har skiftet ut for eksempel en gammel tapestreamer med nyere teknologi uten å ta vare på den gamle streameren. Når man så et halvt år senere har behov for å kopiere tilbake data som ligger på en av de gamle streamerkassettene, har man ikke lenger noen stasjon som kan lese den.

Fotograf: Tim Tadder

Det er ikke nok bare å kjøre regelmessig sikkerhetskopiering. Det må finnes en rutine som sikrer at kopieringen utføres riktig, at kopiene oppbevares trygt, og at det er mulig å legge kopien tilbake hvis man mister data.

Vedlikeholds- og oppdateringsplaner

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vedlikeholds- og oppdateringsplaner (102308)

Maskiner, nettverk og programvare må vedlikeholdes og oppdateres regelmessig. Dette arbeidet bør planlegges.

En virksomhet trenger en vedlikeholdsplan og en oppdateringsplan for å sikre at vedlikehold skjer regelmessig, og for å kunne budsjettere kostnader.

Vedlikeholdsplan

Vedlikeholdsplanen skal sørge for at nødvendig vedlikehold skjer regelmessig, og at noen er ansvarlig for vedlikeholdet, slik at det ikke bare gjøres når det oppstår en feil. For eksempel bør skrivere, tastaturer og mus renses. Det bør kjøres defragmentering av disker, midlertidige filer bør slettes, det må ryddes på serverområder, tilganger må kontrolleres, og så videre.

En vedlikeholdsplan skal inneholde en oversikt over hvilket utstyr som må vedlikeholdes, hva som skal gjøres regelmessig, og hvor hyppig vedlikeholdet skal utføres. Vedlikeholdsplanen bør settes opp på årsbasis.

Oppdateringsplan

Utvikling og slitasje gjør at datamaskiner og utstyr må oppdateres eller skiftes ut med jevne mellomrom. Dette er en kostnad som virksomheten må ha med i sine budsjetter, og innkjøp av nytt utstyr må derfor planlegges god tid i forveien.

Vedlikehold bør planlegges, slik at det ikke bare blir utført når det oppstår feil.

Diskdefragmentering rearrangerer filene som er lagret på harddisken, slik at de lagres sammenhengende. Hensikten er å redusere tiden det tar å laste ned og skrive filer.

Program og operativsystemer må også vedlikeholdes og oppdateres. De fleste programvareprodusenter kommer med serviceoppdateringer etter hvert som de oppdager feil, eller i forbindelse med endringer i operativsystemer eller applikasjoner.

Dette innebærer at du må følge med på om det er kommet oppdateringer for de systemene du har ansvaret for. Det er imidlertid lite hensiktsmessig å løpe rundt og gjøre oppdateringer hver gang det dukker opp noe nytt. Programoppdateringer bør i stedet samles og gjøres regelmessig etter en fastsatt plan.

På denne måten får du bedre kontroll over hvordan de ulike maskinene er konfigurert, og du kan teste at oppdateringene som står for tur, fungerer før de installeres på servere eller brukerens maskiner.

Nye versjoner av kjent – og mindre kjent – programvare lanseres med jevne mellomrom. Windows 7 presenteres her i San Diego i 2012.
Fotograf: Mike Blake

En virksomhet trenger en vedlikeholdsplan og en oppdateringsplan for å sikre at vedlikehold skjer regelmessig, og for å kunne budsjettere kostnader.

Kapasitetsplanlegging

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kapasitetsplanlegging (102309)

Hensikten med kapasitetsplanlegging er å forutse framtidige behov for oppgraderinger, slik at du kan utføre disse før det oppstår problemer.

Kapasitetsplanlegging er også vesentlig når det gjelder budsjettering. Ledelsen i bedriften forlanger normalt å få et budsjett for nødvendige investeringer i forbindelse med den årlige budsjettbehandlingen. Du bør derfor være i stand til å forutse nødvendige oppgraderinger opptil et år i forveien. Uforutsette budsjettoverskridelser blir sjelden godt mottatt i noen virksomhet.

Kapasitetsplanlegging innebærer at man har en rutine for å overvåke de ressursene som kan være en begrensning eller bli en flaskehals. Typiske eksempler er:

- **lagringsplass**: harddiskplass på servere og arbeidsstasjoner samt kapasitet på media for sikkerhetskopiering
- **nettverkskapasitet**: tilstrekkelig hastighet på det interne nettverket og internettilgang
- **serverkapasitet**: serverparkens mulighet til å betjene det forventede antallet brukere og forespørsler (det siste er særlig aktuelt i forbindelse med applikasjonsservere)
- **skriverressurser**: tilstrekkelig kapasitet til å håndtere bedriftens utskriftsvolum

De fleste operativsystemer er utstyrt med verktøy for å måle ressursbelastning. I tillegg finnes det en rekke systemer som er utviklet spesielt for ressursovervåking. Selve informasjonsinnsamlingen er vanligvis automatisert, slik at belastningen på ulike ressurser registreres automatisk på fastsatte tidspunkter.

Fotograf: Corbis

Belastning

Ved kapasitetsplanlegging er man normalt interessert i tre tall, nemlig tall som beskriver

- normal belastning
- maksimal belastning
- forventet belastning

Normal belastning er den belastningen en ressurs blir utsatt for ved normale forhold, mens maksimal belastning er den tyngste belastningen man regner med at ressursen kan bli utsatt for over et kortere tidsrom. Normal og maksimal belasting brukes som utgangspunkt for beregning av forventet belastning.

Når forventet belastning skal beregnes, bruker man gjerne noe som kalles **baselinemetoden**. Metoden innebærer at man først fastsetter et nivå (kalt en baseline) for hva som er normal belastning av en ressurs, for eksempel hva som er normal belastning av virksomhetens internettlinje. Baseline bestemmes ved å logge ressursbruken kontinuerlig over en periode med normal bruk, for eksempel en vanlig arbeidsuke.

Når baseline er fastslått og tallfestet, brukes den som utgangspunkt for videre målinger. Ved å måle belastningen for ressursen regelmessig og sammenligne resultatene med baseline kan man se om belastningen av ressursen minker, øker eller holder seg uforandret.

Dermed kan man etter en stund beregne hvilken kapasitet man vil ha behov for i framtida, og når et eventuelt behov for oppgraderinger vil oppstå.

I tillegg må man selvsagt også ta hensyn til eventuelle andre faktorer som brått kan endre belastningen for en ressurs, for eksempel innføring av nye systemer, oppgraderinger og større endringer i antallet brukere. Når en ressurs oppgraderes, eller når det skjer en betydelig endring i belastningen, må man fastsette en ny baseline, slik at framtidige målinger og beregninger tar hensyn til den nye situasjonen.

Denne typen kapasitetsmålinger gir et forvarsel om når større oppgraderingsjobber, som for eksempel å skifte ut en server eller oppgradere nettverkskapasiteten, må gjøres. På denne måten kan jobbene planlegges god tid i forveien.

På arbeid i serverrommet.

Fotograf: Colorblind

Kapasitetsplanlegging innebærer at man har en rutine for å overvåke de ressursene som kan være en begrensning eller bli en flaskehals.

Driftsavtaler og serviceavtaler

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Driftsavtaler og serviceavtaler (102310)

På grunn av kostnadene til driftsstøtte og for å redusere lønnskostnadene velger mange virksomheter å sette bort driftsstøtten til et eksternt firma som har spesialisert seg på dette.

Det finnes flere firma som tilbyr driftsstøtte enten på timebasis, som periodisk vedlikehold eller som faste driftsavtaler der det eksterne firmaet har ansvaret for alt vedlikehold og IT-drift. Mange firma tilbyr også fjernadministrering (fjerndrift) av virksomhetens nettverk.

De fleste maskinprodusenter og mange programvareleverandører tilbyr i tillegg dedikerte serviceavtaler for sine produkter.

Det finnes også firma som tilbyr såkalte katastrofeløsninger, der virksomhetens servere replikeres til et eksternt driftssenter hver natt. Hvis det skjer noe som gjør at serverne blir ødelagt, for eksempel en brann, kan serverne startes opp igjen fra driftssenteret.

Et vesentlig punkt i serviceavtaler er garantert **responstid**. Typisk vil en avtale garantere at en tekniker er på plass og har startet jobben med å løse problemet innen et spesifisert antall timer etter at problemet er varslet.

At outsourcing-bedriften raskt kan sende en konsulent, er viktig dersom firmaet ditt skal inngå avtale med en ekstern leverandør av IKT-drift. Fotograf: Anthony Redpath

Et vesentlig punkt i serviceavtaler er garantert responstid.

Fagterminologi

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Fagterminologi (102318)

For å kunne kommunisere med leverandører og andre i databransjen er det viktig å kunne faguttrykkene.

Databransjen bruker svært mange faguttrykk og forkortelser. De fleste av disse er engelske ord og uttrykk som ikke har noen entydig norsk oversettelse.

Håndbøker og hjelpefunksjoner for serversystemer og nettverksutstyr finnes vanligvis også bare på engelsk, så du må være forberedt på å lese og forstå mye engelsk.

Det tar tid å lære alle faguttrykkene, og du vil oppleve at det stadig dukker opp nye begreper som du ikke har hørt før.

Ikke fall for fristelsen til å bløffe og late som om du kjenner betydningen av et uttrykk du ikke har hørt før. Du finner en forklaring på de aller fleste datauttrykk i online IT-leksikon som WhatIs.com og Webopedia. I tillegg er den engelske utgaven av Wikipedia et godt oppslagsverk for IKT-begreper og -teknologier.

Lenke: TechTarget WhatIs.com – Engelskspråklig IT-leksikon

Lenke: Webopedia – Engelskspråklig IT-leksikon

Databransjen bruker svært mange faguttrykk og forkortelser. De fleste av disse er engelske ord og uttrykk som ikke har noen entydig norsk oversettelse.

Kurs

Planlegging og gjennomføring av enkle kurs

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Planlegging og gjennomføring av enkle kurs (102406)

Som IKT-servicemedarbeider kan du regne med å bli tatt med i planleggingen av datakurs for de ansatte. Kanskje skal du også være den som skal stå for opplæringen.

Opplæring av de ansatte i bruk av program og datautstyr er svært viktig for at virksomheten skal få fullt utbytte av IKT-investeringene sine.

Alle former for kurs innebærer en kostnad for virksomheten. I tillegg til prisen på selve kurset må bedriften betale for den arbeidstiden som går tapt når de ansatte er på kurs. Virksomheten håper selvsagt å tjene inn igjen dette i form av bedre effektivitet, høyere produktivitet og færre problemer når brukeren behersker IKT-systemene de er kurset i.

Når virksomheten skal sende sine ansatte på kurs, har de som regel følgende alternativer å velge mellom:

- internt kurs med en av sine egne ansatte som instruktør
- internt kurs med ekstern instruktør
- eksternt kurs
- nettbasert kurs

Det er fordeler og ulemper med alle alternativene. Hva som egner seg best, må vurderes fra gang til gang.

Interne kurs har den fordelen at de ansatte ikke behøver å reise bort, og opplæringen kan ofte foregå med utstyr og programversjoner som deltakerne kjenner fra sin egen arbeidssituasjon. En ulempe er at det på en travel arbeidsplass ofte blir forstyrrelser som gjør at det kan være vanskelig for deltakerne å konsentrere seg helt og fullt om kurset. En annen ulempe er at det ofte ikke er noe eget kursrom, slik at man må bruke provisoriske løsninger som møterom eller lignende.

Eksterne kurs har den fordelen at deltakerne ikke risikerer å bli forstyrret av det som skjer på arbeidsplassen, og kurset foregår gjerne i et miljø og med utstyr som er spesielt tilpasset undervisning.

Mange synes også at det er fint å komme bort fra arbeidsplassen en dag eller to, spesielt hvis kurset er kombinert med en eller annen form for sosial aktivitet, som middag på kvelden eller lignende. Ulempen er at slike kurs som regel koster mer, og det kan være vanskeligere å koble det man gjør på kurset, til sin egen arbeidssituasjon fordi kursmiljøet ikke ligner på det arbeidsmiljøet man er vant til.

Nettbaserte kurs er en rimelig form for opplæring, men krever høy motivasjon hos deltakerne. Nettkurs er gjerne lagt opp som selvstudium. Fordelen med det er at man kan arbeide i sitt eget tempo og prioritere det man har størst behov for å lære. Ulempen er at man i stor grad er overlatt til seg selv og ikke har noen instruktør som kan hjelpe eller forklare når man står fast.

Det er ofte en fordel å arrangere kurs i kursrom som er spesielt tilrettelagt for dette.
Fotograf: C. Devan

Fjernundervisning via Internett blir mer og mer vanlig, også som tilbud til ansatte som har behov for å oppgradere kunnskapen sin på arbeidsplassen.
Fotograf: Greg Vote

Alle former for kurs innebærer en kostnad for virksomheten. I tillegg til prisen på selve kurset må bedriften betale for den arbeidstiden som går tapt når de ansatte er på kurs.

Kartlegge opplæringsbehovet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kartlegge opplæringsbehovet (102417)

Mange virksomheter kaster bort mye tid og penger på kurs som deltakerne har lite igjen for, fordi de slurver med planleggingen og forarbeidet.

Å sende ansatte på datakurs gir ingen garanti for at de blir flinkere til å bruke datamaskinen, eller at de blir mer effektive. Hvis kurset ikke er tilpasset deltakerne, kan det fort være bortkastet tid og i verste fall føre til mer frustrasjon og usikkerhet hos brukerne.

Et vellykket kurs krever derfor at du først kartlegger det faktiske behovet. Det vil si

- hva brukerne egentlig har behov for opplæring i
- hvilke behov den enkelte har
- hvilket nivå den enkelte brukeren er på

Du kan benytte deg av flere kilder for å innhente den informasjonen du trenger:

- et enkelt spørreskjema som brukerne kan svare på
- statistikk fra supportlogger som viser hvilke problemer brukerne oftest kontakter support for å få hjelp med
- brukermønsterundersøkelser, det vil si undersøkelser som viser hvordan og i hvilken grad ansatte bruker IKT-systemene og utnytter funksjonaliteten

Som regel vil det vise seg at det er behov for flere ulike kurs på forskjellige nivå, og du må derfor vurdere hvilke behov som er mest kritiske, og hva slags kurs som vil ha størst nytteverdi. Gjør du jobben ordentlig, vil du kunne sette opp en opplæringsplan som tar hensyn til de ansattes ulike behov.

Husk å kartlegge kursdeltakernes behov *før* kurset – det er for sent når kurset har startet.
Fotograf: C. Devan

Hvis kurset ikke er tilpasset deltakerne, kan det fort være bortkastet tid og i verste fall føre til mer frustrasjon og usikkerhet hos brukerne.

Lag en enkel opplæringsplan

La oss se på et eksempel. Anta at det er behov for et Excel-kurs i virksomheten du jobber i. Når du undersøker behovet nærmere, oppdager du at en del brukere kan svært lite om Excel og derfor trenger et grunnkurs.

Andre brukere er mer drevne og har behov for å lære litt mer avanserte funksjoner. Mange virksomheter vil imidlertid aldri komme lenger enn til å konstatere at man har behov for Excel-opplæring.

Deretter vil de kjøpe et kurs som de sender alle brukerne på. Dette kurset vil enten være for avansert for dem som kan lite, for enkelt for dem som kan mye, eller noe midt imellom som ingen egentlig har noe utbytte av.

Hvis du har kartlagt behovene på en skikkelig måte, kan du lage en opplæringsplan der de som kan lite, får et grunnkurs først, slik at alle kan delta på et videregående kurs etterpå. Eksempelet er enkelt, men dessverre er slike elementære planleggingsfeil svært vanlige.

Bestemme opplæringsform, kursinnhold og omfang

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Bestemme opplæringsform, kursinnhold og omfang (102429)

Når du har oversikt over hvilket behov brukerne har for opplæring, må du bestemme opplæringsform, kursinnhold og lengde på kurset.

Opplæringsform

Det er mye du bør tenke igjennom når du skal velge opplæringsform:

- Hvor mange deltakere skal kurses?
- Bør opplæringen gjøres på arbeidsplassen eller i et eksternt kurslokale?
- Bør opplæringen gjøres samlet for en stor gruppe, i mindre grupper eller individuelt?
- Skal deltakerne ha pc tilgjengelig under hele eller bare deler av kurset?
- Bør hver deltaker ha en egen pc, eller er det en fordel at to deler en maskin, slik at de kan samarbeide?
- Bør deltakerne bruke sin egen pc eller en kurs-pc?

Hvis det er få deltakere og det er stor forskjell på behovene, kan det være mer effektivt å gi personlig opplæring til den enkelte.

Hvis det er mange som skal kurses samtidig, er det ikke sikkert at deltakerne bør ha pc tilgjengelig hele tiden. Det kan være bedre at alle følger med mens du gjennomgår funksjonene. Etterpå kan de prøve selv og jobbe med oppgaver mens du kan gå rundt og hjelpe dem som har problemer.

Kursinnhold

Generelt gjelder regelen om at det er bedre å lære noen få ting godt enn mange ting dårlig. For mye informasjon på for kort tid gir alltid et dårlig resultat. Spesielt er dette viktig for nybegynnerkurs. Forsøk å legge vekt på de mest brukte og viktigste funksjonene, og bruk heller mer tid på disse.

Eksempler og oppgaver som du skal bruke på kurset, bør i størst mulig grad være relatert til den arbeidssituasjonen deltakerne møter til daglig. Da er det lettere for deltakerne å se nytteverdien av det de lærer, og forstå hvordan de kan bruke ulike funksjoner.

Lengden på kurset

Lengden på kurset er avhengig av kursinnholdet, hvor mye som skal gjennomgås, og hvor vanskelig det er. Når du skal beregne lengden på kurset, må du også ta hensyn til at deltakerne må få anledning til å jobbe med praktiske oppgaver underveis.

Et datakurs bør ikke være for langt. Det kan være bedre å holde to halvdagskurs enn ett heldagskurs.

Tenk også på at det som regel tar lengre tid jo flere deltakere det er på kurset, fordi det blir flere spørsmål og flere som trenger hjelp.

Tenk igjennom på forhånd i hvilken grad det kan være nyttig at deltakerne samarbeider om oppgaver på kurset.
Fotograf: C. Devan

Del opp kursene i mindre deler, så risikerer du ikke at kursdeltakerne mister konsentrasjonen underveis.
Fotograf: Serge Kozak

Generelt gjelder regelen om at det er bedre å lære noen få ting godt enn mange ting dårlig.

/
http://ndla.no/nb/node/

Lage informasjon om kurset

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Lage informasjon om kurset (102436)

Når opplæringsform, kursinnhold og lengden på kurset er bestemt, må deltakerne få informasjon om kurset. Denne informasjonen skal sendes ut i forkant av kurset og skal både forberede og motivere deltakerne til kurset.

Hvor omfattende informasjonen bør være, er avhengig av hvor omfattende kurset er, men du bør vurdere følgende:

- **En begrunnelse for hvorfor kurset holdes:** Det er viktig at alle deltakerne forstår hva som er hensikten med kurset, og hvorfor det er behov for det.
- **En oversikt over hvem som bør delta:** Hva slags kunnskapsnivå, arbeidssituasjon og lignende har deltakerne? Dette gir deltakere mulighet til å vurdere om kurset er riktig for dem.
- **En beskrivelse av hva som er målet med kurset, og hvilken nytteverdi det har både for deltakerne og for virksomheten** Et kurs bør ha et klart mål som både virksomheten og deltakerne forstår og kan forholde seg til.
- **En detaljert oversikt over kursinnholdet:** En kursplan bør gjøres kjent på forhånd.
- **Et forslag til hvordan deltakerne best kan forberede seg før kurset:** Hva bør de kunne før kurset starter? Hva bør de lese på forhånd? Hva bør de ha med seg? Hvis kurset har lærematerіell, kan det godt sendes til deltakerne sammen med kursinformasjonen, slik at deltakerne kan gjøre seg kjent med det på forhånd.
- **En oversikt over hvordan kurset vil bli fulgt opp:** Dette kan være informasjon om eventuelle videre kurs, hvordan du har tenkt å evaluere kurset, oppgaver eller øvelser som deltakerne må regne med å gjøre etter at kurset er over, og lignende.
- **Hvis kurset er eksternt, trenger du også en beskrivelse av kursarrangøren og gjerne litt om instruktøren** Videre bør du gi informasjon om praktiske ting som parkering, lunsj og så videre. Ta gjerne med et bilde av lokalene og instruktøren også.

Kursplanen bør være ganske detaljert. Skal du for eksempel holde et kurs i tekstbehandling, bør kursplanen inneholde en oversikt over hvilke funksjoner du kommer til å gjennomgå.

Det kan også være en fordel å si noe om vanskelighetsgrad og hvor grundig hvert tema vil bli behandlet. Videre bør kursplanen vise hvor mye tid som blir satt av til oppgaveløsing og øvelser. Hvis kurset har en lærebok eller annet lærematerіell, bør kursplanen inneholde referanser til dette for de enkelte temaene.

Hvis du bruker en ekstern kursarrangør, er det viktig at du samarbeider med denne om kursplanen. Arrangøren må også få en kopi av den informasjonen du sender ut til deltakerne, slik at de vet hva deltakerne og virksomheten forventer.

Et kurs bør ha et klart mål som både virksomheten og deltakerne forstår og kan forholde seg til.

Holde kurset

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Holde kurset (102440)

Nøkkelen til å holde et vellykket kurs er å være godt forberedt. Selv om du kan det programmet eller systemet du skal holde kurs i, godt selv, må du tenke igjennom hvordan du best kan lære det bort til andre. Husk at deltakerne er der for å lære, ikke for at du skal vise hvor flink du er.

Jobb deg igjennom hele kursinnholdet på forhånd, og tenk på i hvilken rekkefølge du bør vise ulike funksjoner, og hvordan du skal forklare dem. Noter gjerne stikkord, slik at du ikke glemmer viktige poeng.

Tenk også igjennom hva du eventuelt skal vise på skjerm eller med projektor. Hvis du skal forklare mye teori, kan en PowerPoint-presentasjon være en god støtte, men hvis du skal vise funksjoner i et program, kan det være bedre å ha programmet framme på skjermen.

Hvis deltakerne skal lære mange funksjoner i programmet, er det lurt å lage oppskrifter på papir som deltakerne kan følge. Da slipper de å notere underveis og kan følge oppskriftene når de skal prøve funksjonene på egen hånd etter kurset.

Du bør også lage alle oppgaver og øvelser deltakerne skal jobbe med, ferdig på forhånd.

Tenk igjennom hva du skal vise på skjerm, før kurset starter.
Fotograf: Corbis

Beregne tiden

Det kan være vanskelig å beregne hvor lang tid det vil ta å komme igjennom det lærestoffet du har planlagt. Det er mulig du må forklare det samme flere ganger, og det kan være at deltakerne har spørsmål som du må svare på. Men du kan også risikere at det går mye raskere enn du hadde tenkt – for eksempel hvis deltakerne kan mye fra før.

Du bør derfor forberede deg på å gå igjennom litt mer enn det du regner med at du rekker, men legge det opp slik at du gjennomgår det viktigste først og det minst viktige til sist. Da gjør det ikke så mye om du får knapt med tid og må kutte ut noe.

Sørg for at alt er i orden før kurset starter

I god tid før kurset starter, må du sjekke at du har alt du trenger, og at alt fungerer som det skal. Det er frustrerende både for deg og for deltakerne hvis den første timen går med til å få maskiner, program, projektor eller annet til å fungere.

Sjekk at

- alle maskiner fungerer som de skal
- det er mulig å logge seg inn
- programmene som skal brukes, starter og virker slik de skal
- maskinene har nettilgang
- projektoren fungerer
- presentasjoner eller annet som du skal vise på skjermen, er i orden
- du har alt kursmateriell som skal brukes, eventuelle øvingsfiler og så videre

Takle nervøsitet

Det er helt vanlig å bli litt nervøs eller stresset når man skal holde kurs, spesielt hvis det er mange deltakere du ikke kjenner godt, og du ikke er vant til å holde kurs.

Den beste måten å håndtere nervøsitet på er å være godt forberedt. Nervøsiteten er gjerne mest intens de første minuttene etter at du har startet kurset. Hvis du vet at du antakelig blir nervøs, er det lurt om du forbereder de første fem minuttene ekstra godt og øver deg på det du skal si og gjøre.

Forsøk ikke å stresse når du snakker. Pust dypt, og snakk rolig og tydelig. Hvis du føler at nervøsiteten tar overhånd, kan du godt fortelle deltakerne at du er nervøs. Da trenger du ikke lenger å anstrenge deg for å skjule nervøsiteten, og kroppen slapper mer av.

Sjekk at alt utstyret fungerer, før kurset starter.
Fotograf: Holger Scheibe

Gjennomføre

Etter at du har ønsket velkommen og presentert deg selv, bør du starte kurset med en oversikt over hva du kommer til å gjennomgå, og hvordan du har lagt opp kurset med hensyn til øvelser, oppgaver og bruk av maskiner underveis.

Når deltakerne har tilgang til pc på kurset, vil mange gjerne prøve funksjonene på sin maskin samtidig som du viser og forklarer dem. Det fører lett til at de går glipp av noe du viser, eller at de roter seg bort i programmet, slik at du må avbryte for å hjelpe dem tilbake.

For å unngå for mange avbrudd kan det være lurt at du forklarer en funksjon først og så gir deltakerne noen minutter til å prøve den før du går videre.

Når du viser funksjoner i et program, bør du også forklare hensikten med dem og bruke eksempler, slik at deltakerne forstår både hvordan funksjonene brukes, og hva de kan bruke dem til.

Unngå å vise for mange måter å gjøre samme ting på. Mange program har flere alternativer for den samme funksjonen. I de fleste Office-pakker finnes for eksempel de mest brukte funksjonene både som et menyvalg, som en knapp, som en hurtigtast og på en høyreklikkmeny.

Du bør avslutte kurset med en oppsummering av hva dere har gjennomgått.

Dersom du skal holde kurs for en større forsamling, kan det være lurt å gjøre seg kjent med kurslokalet på forhånd.
Fotograf: Corbis

Nøkkelen til å holde et vellykket kurs er å være godt forberedt.

Alternativer til kurs

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Alternativer til kurs (102445)

Et alternativ til å holde et vanlig kurs er å arrangere en *workshop.*

Workshop kan oversettes med «verksted», og er en betegnelse på et kurs der læringen skjer gjennom praksis, samarbeid og deling av informasjon.

Deltakerne jobber sammen i grupper og lærer av hverandre ved å løse oppgaver. Instruktørens jobb er å sette gruppene i gang og hjelpe til underveis.

Workshops gir større fleksibilitet ved at grupper kan jobbe med ulike oppgaver avhengig av kunnskapsnivå og behov.

Det er også mulig å kombinere et vanlig kurs med en workshop, for eksempel ved å holde et vanlig kurs før lunsj og en workshop etter lunsj.

Workshops der noen få ansatte samarbeider om å lære ny teknologi, kan fungere godt som et alternativ til vanlige kurs. Fotograf: Annemor Larsen

Evaluere og følge opp kurset

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Evaluere og følge opp kurset (102447)

Når kurset er ferdig, må det evalueres for å se om du har nådd målene dine.

Etter at kurset er ferdig, må det evalueres. Det bør gjøres i to omganger. I den første evalueringen, som bør skje med en gang kurset er ferdig, får deltakerne si sin mening om instruktøren, kursinnholdet og selve gjennomføringen.

Neste evaluering bør gjøres to–fire uker etter kurset. Da bør du spørre deltakerne om nytteverdien av kurset. Har de fått bruk for noe av det de lærte? Har de færre problemer nå enn tidligere? Føler de at målet for kurset ble nådd? Har de fått anledning til å følge opp innholdet slik det var planlagt?

Hvis det er mulig, bør evalueringene være anonyme.

Etter at evalueringene er avsluttet, gjennomgår du resultatene for å se om du har nådd de målene du hadde for kurset. Tilbakemeldingene fra deltakerne er viktige, men du kan også se på om det har skjedd noen endring i antallet henvendelser fra brukerne, eller om programmet kurset gjaldt, nå brukes i større grad. Hvis kurset ikke har gitt de resultatene du forventet, må du se på innholdet og gjennomføringen for å finne ut hva du bør gjøre annerledes neste gang.

Hvis kurset ikke har gitt de resultatene du forventet, må du se på innholdet og gjennomføringen for å finne ut hva du bør gjøre annerledes neste gang.

Noen vanlige feil ved planlegging og gjennomføring av kurs

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Noen vanlige feil ved planlegging og gjennomføring av kurs (102448)

Mange virksomheter slurver med kvalitetskontrollen av opplæringen de tilbyr de ansatte, og de ansatte er ikke alltid like flinke til å si fra.

Det er mange faktorer som kan føre til at et kurs eller kursopplegg ikke gir den effekten du hadde tenkt:

- **Kurset er for generelt i forhold til deltakernes behov**. Brukere har ofte svært spesifikke behov for opplæring. De trenger kurs i bestemte program og gjerne også bestemte funksjoner i programmene. Hvis kurset blir for generelt, er det lite deltakerne kan bruke direkte i sin arbeidssituasjon.
- **Kurset er for spesielt i forhold til deltakernes behov (feil innhold)** Et kurs der innholdet er rettet mot et bestemt tema, er som regel bedre enn et generelt kurs, men det er selvsagt avhengig av at innholdet faktisk stemmer med det deltakerne har behov for å lære om.
- **Kurset tar ikke hensyn til deltakernes kunnskapsnivå**. Deltakere på et kurs har som regel forskjellig kunnskapsnivå, og kurset må ta hensyn til dette. Legg merke til at et kurs med for enkelt innhold er like bortkastet som et kurs med for avansert innhold.
- **Kursinnholdet er for omfattende**. Den kanskje vanligste feilen er at man forsøker å pakke for mye informasjon og for mange funksjoner inn i ett kurs og på for kort tid. Resultatet er at deltakerne mister oversikten, og at læringen blir begrenset.
- **Deltakerne er ikke tilstrekkelig motivert**. Alle som har forøkt å lære noe, vet at man må være motivert for å klare det. Hvis deltakerne blir sendt på kurs uten å forstå hvorfor, eller uten å forstå hva de skal bruke det de lærer, til, har kurset liten hensikt.
- **Instruktøren kan for lite om deltakernes arbeidssituasjon**. Ansatte i en virksomhet har gjerne spesifikke behov knyttet til den jobben de har. Hvis instruktøren har for liten kjennskap til den arbeidssituasjonen deltakerne møter til daglig, kan det være vanskelig å forstå de problemene og behovene de har.

Husk å tilpasse kurset til den ansattes kompetansenivå. En superbruker har helt andre behov enn andre ansatte. Fotograf: Mike Schröder

Mange virksomheter slurver med kvalitetskontrollen av opplæringen de tilbyr de ansatte, og de ansatte er ikke alltid like flinke til å si fra.

Oppgaver

Presentasjon av selvvalgt tema innen IKT

Forfatter: Jan Frode Lindsø
Presentasjon av selvvalgt tema innen IKT (133433)

Denne oppgaven lar elevene få prøve seg på grunnleggende presentasjonsteknikk. Den utfordrer elevene til å lage og forberede en presentasjon, og gir øving i å presentere for et publikum.

Målet med denne oppgaven er å få grunnleggende ferdigheter i presentasjonsteknikk, og for å øve deg på å snakke foran et publikum. Du skal velge et tema du vil presentere som du interesserer deg for innen IKT, og hva som fikk deg til å bli interessert i det.

Du kan ikke velge konkrete spill, applikasjoner og plattformer som for eksempel Battlefield, Photoshop, Facebook og lignende, men generelt om teknologien (sosiale medier, dataspill, bildebehandling osv.).

Noen viktige stikkord som bør tas med er:

- Bakgrunnshistorie
- Positive-/negative-sider
- Hvorfor er du interessert i dette temaet?
- Hvordan bruker man det?
- Er det brukervennlig?
- Ta med noen konkrete eksempler (men husk at dette ikke skal dominere presentasjonen).

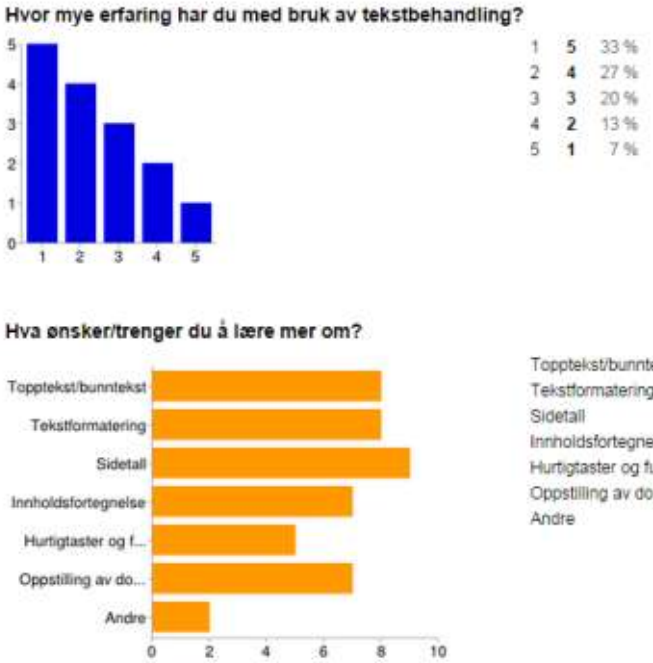
Utover dette står du fritt til å velge hva du mener er viktig å ta med i en slik presentasjon. Presentasjonen skal være på ca. 10 min. og skal presenteres for resten av klassen. Temaet du skal skrive om må godkjennes av læreren før du begynner,

Kursplanlegging

Forfatter: Jan Frode Lindsø
Kursplanlegging (137396)

I denne oppgaven skal du øve deg på å planlegge kurs basert på innsamlet data.

Under ser du et utdrag fra et spørreskjema som er utsendt i forkant av et kurs i tekstbehandling. Ta utgangspunkt i innsamlet data, og sett opp et forslag til en kursplan.



Resultat spørreundersøkelse

Kunnskapsnettverk

Innledning til kunnskapsnettverk og kunnskapsutvikling

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innledning til kunnskapsnettverk og kunnskapsutvikling (107651)

Virksomheter er opptatt av kunnskap og vil gjerne fremstå som kunnskapsbedrifter eller kunnskapsorganisasjoner som hele tiden utvikler seg.

Du har sikkert hørt eller lest at vi lever i et ”informasjonssamfunn”. Men kunnskap er mer enn informasjon. Kunnskap innebærer at du også vet hvordan du skal bruke tilgjengelig informasjon i praksis. Uten kunnskap har ikke informasjonen noen egentlig verdi.

Forfatteren og økonomen Peter Drucker oppsummerte det på følgende vis: ”*Informasjon blir bare kunnskap i hendene på noen som vet hva de skal gjøre med den.*”

Den vanligste formen for kunnskapsutvikling i virksomheter er å organisere kurs for de ansatte. Det er i tråd med tradisjonell tankegang om hvordan vi lærer, men dette er ikke alltid den beste måten å utvikle kunnskap på.

Det er gjort mange undersøkelser om læring på arbeidsplassen som konkluderer med at de beste måtene å lære på er

- å utføre oppgaver selvstendig
- å utføre oppgaver sammen med kollegaer
- å snakke sammen og diskutere med kollegaer

Å utføre arbeid på egen hånd kan ofte være den beste måten å lære på.
Fotograf: Berit Roald

"Informasjon blir bare kunnskap i hendene på noen som vet hva de skal gjøre med den."
– Peter Drucker

Det betyr ikke at kurs ikke har noen betydning. Men i en virksomhet skjer mye av den viktigste kunnskapsutviklingen gjennom arbeid med praktiske oppgaver, sosiale relasjoner, kunnskapsnettverk og i situasjoner hvor det er mulig å samarbeide med kollegaer og observere hvordan kunnskapen brukes.

Læring og kunnskapsutvikling er kontinuerlige prosesser i alle bransjer og virksomheter, spesielt innenfor IKT. Den teknologiske utviklingen går fort, og som IKT-servicemedarbeider må du regne med å bruke en god del tid på å holde deg oppdatert. Det er derfor lurt å sette din egen læring og kunnskapsutvikling i system.

Personlige og profesjonelle læringsnettverk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Personlige og profesjonelle læringsnettverk (107653)

For å sette din egen læring og kunnskapsutvikling i system kan du bygge deg ditt eget digitale personlige læringsnettverk.

Vi kan skille mellom formell og uformell læring. Formell læring er systematisk læring som avsluttes med en evaluering, mens læring som ikke har noen evaluering, kalles uformell. Skole og kurs er de vanligste eksemplene på formell læring, mens det du lærer på egen hånd, ved for eksempel å lese, delta på seminarer, jobbe sammen med andre, løse nye problemer, osv., er uformell læring.

Det meste av læringen i en arbeidssituasjon er uformell. Men selv om uformell læring ikke følger noen bestemt plan eller har noen eksamen, er det fortsatt mulig å sette den i system. En måte å gjøre det på er å organisere et digitalt **personlig læringsnettverk** (PLN).

Når vi sier digitalt nettverk i denne sammenhengen, mener vi ikke et vanlig datanettverk. Det er de menneskene du kommuniserer med på Internett, og de ressursene du bruker for å holde deg oppdatert, lære og utvikle deg, som er ditt digitale personlige læringsnettverk. Sosiale medier og nettbaserte Web 2.0-verktøy gir nesten ubegrensede muligheter for informasjonsinnhenting, kommunikasjon og læring.

I noen sammenhenger brukes også forkortelsen PLN om **profesjonelt læringsnettverk**. Et profesjonelt læringsnettverk er et nettverk for personer innenfor et bestemt fagfelt eller yrkesgruppe. En virksomhet kan organisere et profesjonelt læringsnettverk for sine ansatte.

Bygge et personlig læringsnettverk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Bygge et personlig læringsnettverk (107657)

Et digitalt personlig læringsnettverk er personlig. Derfor finnes det ikke noen fasit på hvilke ressurser du bør bruke, og hvordan du bør bruke dem.

Et digitalt personlig læringsnettverk har to deler:

1. et sett med tjenester og verktøy på Internett
2. en systematisk plan for hvordan tjenestene og verktøyene skal brukes til læring

Hvilke tjenester og verktøy du vil inkludere i ditt PLN, er opp til deg. Et læringsnettverk er heller ikke noe du bygger en gang for alle. Et godt nettverk utvikler seg hele tiden. Nye tjenester og mennesker kommer til mens gamle forsvinner.

Det er mange mulige kilder til informasjon som du kan inkludere. Du kan for eksempel

- bli medlem av faggrupper på sosiale medier. Det finnes mange grupper på Facebook, LinkedIn og andre sosiale medier for bestemte interesser og yrkesgrupper.
- følge kunnskapsrike eller profilerte personer på Twitter
- abonnere på fagblogger
- abonnere på RSS-strømmer fra interessante nettsider
- følge interessante YouTube-kanaler
- bli medlem av fagforumer

Men målet er ikke å samle flest mulig ressurser. Husk at du også må kunne følge opp de ressursene du inkluderer. Til det trenger du en plan. Tenk gjennom hvilken kunnskap og informasjon du har behov for, hvordan du skal bruke nettverket ditt, og hvilke mennesker du gjerne vil ha kontakt med.

Å inkludere for mange ressurser kan føre at den kunnskapen du faktisk har behov for, drukner i ”støy”. Målet med et digitalt personlig læringsnettverk er at du skal

- vite hvem som har den kunnskapen du trenger
- vite hvor du finner den informasjonen du trenger
- få ny informasjon som du ikke visste at du trengte

Deling av informasjon

Utgangspunktet for Internett var at det skulle bli enklere for forskere på universiteter i ulike byer og land å dele informasjon med hverandre. Denne Delingskulturen er fortsatt en av de sterkeste drivkreftene for mange av de mest brukte tjenestene på nettet i dag. Tjenester som Wikipedia og sosiale medier som Facebook og YouTube er i sin helhet basert på at det er brukerne selv som produserer innholdet og gjør det tilgjengelig for andre.

Med venner og bekjente deler vi gjerne villig vekk, og for å få til kunnskapsdeling og læring i en virksomhet er det viktig å bygge en tilsvarende god delingskultur med kollegaer og andre kontakter.

Skill mellom jobb og privatliv

Fotograf: Daniel Koebe

Et RSS-ikon

Fotograf: Martin Diller

Et PLN handler ikke bare om tilgang til informasjon. Kommunikasjon er like viktig, og da må du bidra selv også.

Wikipedia er bygget opp av brukere over hele verden.

Fotograf: Wikipedia

På samme måte som vi skiller mellom arbeidstid og fritid, kan det være lurt å skille mellom jobb og privatliv på Internett også.

Mange velger å ha to kontoer på sosiale medier som Facebook og Twitter. En for familie og venner og en annen for kollegaer og annet som har med jobben å gjøre.

Lenker

7 forutsetninger for en god delingskultur

Kan jeg stole på deg?

Se gjerne også på kommentarene til disse blogginnleggene.

Start med en gang

Du trenger ikke å vente til du er ferdig med skolen før du begynner å bygge et digitalt personlig læringsnettverk. Det er bare å gå i gang. Opprett nødvendige kontoer, legg til ressurser som du synes er interessante, inviter andre i klassen til å være med i nettverket ditt.

Tenk på at dere når dere er ferdig på skolen, går videre til ulike arbeidsplasser. Hvis dere allerede har et nettverk på plass, kan dere fortsette å utveksle informasjon og gjennom hverandre få kontakt med flere i bransjen.

Et godt nettverk gir også en mulighet til å ”markedsføre” din egen kompetanse. Gode ressurspersoner blir lagt merke til, og det kan gi deg både lærlingplass og jobb.

Kunnskapsnettverk i virksomheter

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kunnskapsnettverk i virksomheter (107659)

En virksomhet kan lage sitt eget interne kunnskaps- og læringsnettverk.

En virksomhet kan benytte dataverktøy og Internett til å lage sitt eget interne kunnskapsnettverk. Det er særlig aktuelt i store virksomheter og i virksomheter som er geografisk spredt. For eksempel kjedeforetak og virksomheter med kontorer i flere landsdeler eller land.

Ressursene i nettverket vil i mange tilfeller være de samme som i et personlig læringsnettverk, men begrenset slik at bare de som er tilknyttet virksomheten, har tilgang. For eksempel en lukket Facebook-gruppe, en egen YouTube-kanal, et intranett, kommunikasjonsprogrammer som Skype, eller verktøy for samarbeid og samskriving som Google Dokumenter.

En viktig del av kunnskapsdeling i en virksomhet er å dokumentere og gjøre tilgjengelig løsninger på problemer. Dette lærer du mer om i det egne kompetansemålet "Dokumentere og gjøre tilgjengelig løsninger på problemer".

På Google Dokumenter kan du velge å dele dokumenter og regneark med andre, og benytte verktøyet til samskriving. Skjermdump fra Google Docs.
Opphavsmann: Google

RSS

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
RSS (107661)

Å følge med på mange nettsteder og blogger kan fort bli tidkrevende hvis du stadig må besøke sidene for å se om det er kommet noe nytt der. En enkel løsning på dette problemet er å benytte RSS.

RSS (Really Simple Syndication) er et standardisert format for distribusjon av nyheter, artikler og oppdateringer fra nettsteder. Enkelt forklart er RSS en teknologi som fortløpende sender deg overskriftene og et kort sammendrag av de siste nyhetene fra de nettstedene du vil følge med på.

Dette kalles for en RSS-strøm (RSS-feed), og denne strømmen samles slik at du kan lese den i en RSS-leser. Når det dukker opp en artikkel som ser interessant ut, er det bare å klikke på den i RSS-leseren for å lese hele.

For å bruke RSS trenger du en RSS-leser. Nettbaserte lesere som Google Leser (Google Reader) og Bloglines er populære, men det er mange alternativer. Det finnes også RSS app-er for mobiltelefoner og nettbrett. For eksempel Flipboard.

Lenke: RSS – Spar tid, bli varslet om ny informasjon

Lenke: Slik virker RSS

Med RSS kan du lage din egen personlige "avis" med informasjon og nyheter som interesserer deg.

Google Reader

Når du har funnet en RSS-leser du vil bruke, kan du begynne å abonnere på RSS-strømmer. Når et nettsted tilbyr en RSS-strøm, vises det med et oransje symbol.

RSS-ikoner

Ved å klikke på symbolet får du spørsmål om hvordan du vil motta nyhetsstrømmen. Nettstedet vil da begynne å sende deg oppdateringer når det legges ut nye artikler. Du kan når som helst stoppe et RSS-abonnement som ikke interesserer deg lenger fra RSS-leseren.

Oppgaver

Skap et personlig læringsnettverk

Forfatter: Jan Frode Lindsø
Skap et personlig læringsnettverk (138278)

I denne oppgaven lærer du å bygge et personlig læringsnettverk (PLN).

Det finnes mange måter å bygge et personlig læringsnettverk på. Ett alternativ kan være å bruke Twitter. Her er mange mennesker fra ulike fagmiljøer representert.

For å bruke Twitter må du ha en brukerkonto. Når denne er opprettet, kan du begynne å følge personer. For å finne personer innen din egen bransje kan du begynne med å søke på fagspesifikke begrep (for eksempel IKT, IKT-servicefag osv.). På denne måten vil du finne samtaler der disse begrepene er i bruk. Du kan deretter se om det er noen du ønsker å følge. Ofte merker man disse begrepene med såkalte hashtags, på norsk også kalt emneknagger (for eksempel #ikt). Klikk her for å få hjelp og innføring i Twitter.

På Twitter er det lurt å følge personer du deler interesser og fagfelt med. Du kan også lage lister over spesifikke grupper med personer (for eksempel lærere, IT-ansvarlige, designere osv.).

Oppgaver:
1. Opprett en konto på Twitter.
2. Finn interessante personer, og følg disse.
3. Kommuniser med andre i klassen ved å bruke ulike hashtags (emneknagger).

Lag en digital CV

Forfatter: Jan Frode Lindsø
Lag en digital CV (138337)

I denne oppgaven lærer du å lage en digital CV som du kan bruke i ditt personlige læringsnettverk.

LinkedIn er et sosialt nettverk som har likhetstrekk med tradisjonelle sosiale nettverk, men det brukes i hovedsak til å samle forretningsforbindelser. LinkedIn har også vokst seg til å bli en stor aktør innen rekruttering, og inneholder mange jobbutlysninger.

På LinkedIn kan du opprette din egen profil og din egen CV. Den CV-en kan du legge ved når du søker på jobber senere. Det kan også være at noen i nettverket ditt leter etter nettopp din kompetanse. På den måten kan LinkedIn være et bidrag til ditt personlige læringsnettverk.

Oppgaver:
1. Opprett en konto på LinkedIn.
2. Legg inn hele klassen din som kontakter.

Hjelp og veiledning

Informasjonskilder

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Informasjonskilder (107670)

Som IKT-servicemedarbeider er du avhengig av å ha tilgang til teknisk informasjon for å kunne løse mange av de problemene som oppstår. Erfaring er selvsagt viktig, men det vil alltid dukke opp problemer du ikke har sett tidligere.

Selv om en oppgave eller et problem kan være nytt for deg, er det svært sjelden at det dukker opp helt nye feil med maskin- eller programvare. Som regel er problemet kjent av produsenten eller andre brukere, og løsningen er dokumentert. Hvor raskt du kan løse et problem, er derfor ofte et spørsmål om hvor raskt du er i stand til å finne fram til denne informasjonen. Det finnes mange ulike informasjonskilder du kan bruke.

Brukerhåndbøker

Med nesten alle typer datautstyr følger det med en brukerhåndbok – enten som en trykt bok eller i et digitalt format. De fleste leverandører har også digitale versjoner av brukerhåndbøkene på nettsidene sine. I tillegg til teknisk informasjon inneholder brukerhåndboken gjerne grunnleggende feilsøkingsinformasjon og svar på vanlige spørsmål, basert på produsentens erfaring med hva kundene ofte spør om og har problemer med.

Det er derfor en god idé å bygge opp et lite bibliotek med de håndbøkene som følger med det utstyret du har ansvaret for.

Lokal erfarings- eller supportdatabase

En viktig del av det å administrere IKT-support er å dokumentere de feilene og problemene som oppstår, og hvordan de ble løst. Etter en tid vil en slik erfaringsdatabase inneholde mye verdifull informasjon om de systemkombinasjonene virksomheten har, og de spesielle feilene og problemene man har erfart tidligere.

Fotograf: Kerstin Mertens

Dokumenter alltid de løsningene du har funnet fram til, og ta vare på det for framtidig bruk.
Fotograf: Berit Roald

Her kan du finne et eksempel på en side med kontaktinformasjon hos Microsoft.

Du tenker kanskje at du vil huske hvordan et bestemt problem ble løst, men når et tidligere problem dukker opp igjen et par år senere, har man som regel glemt detaljene. Tenk også på at du sikkert ikke kommer til å ha den samme jobben for all framtid, og den erfaringen du bygger opp og dokumenterer, er uvurderlig for den som skal overta jobben en gang i framtiden.

Leverandørens supportsenter eller supportdatabase

Alle IT-leverandører har en egen supportavdeling for å betjene sine kunder. Når du støter på et nytt problem med utstyr fra en bestemt leverandør, er det naturlig å benytte seg av leverandørens tjenester.

Du bør ha en liste med telefonnummer til supporttelefonen for de maskinene og programmene du har ansvaret for. Listen kan i tillegg til telefonnummer og eventuell kontaktperson også inneholde en oversikt over hvilken informasjon du vet leverandøren vil be om når du ringer, slik at du kan ha den klar. Typiske eksempler på slik informasjon kan være serienummer, operativsystemversjon, biosversjon, lisensnummer og så videre.

Mange leverandører gir også kundene direkte adgang til sine egne erfaringsdatabaser via Internett, slik at man selv kan søke i og hente ut den informasjonen som supportsenteret baserer seg på.

> Det vil alltid dukke opp problemer som du ikke har sett tidligere.

Internett som supportressurs

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Internett som supportressurs (107677)

Internett er den viktigste og mest effektive informasjonskilden for IKT-servicemedarbeidere. De fleste problemer som oppstår, er allerede kjent av enten produsenten eller andre brukere, og mulige løsninger er dokumentert på Internett.

Produsentenes nettsider

Produsenten eller leverandørens nettsider er det naturlige stedet å starte informasjonssøkingen, og alle større leverandører har egne supportsider tilgjengelig på Internett. Kvaliteten varierer imidlertid svært når det gjelder både innhold og søkemuligheter. I tillegg er ikke alltid grensesnittet like intuitivt.

Mange leverandører har koblet supportsidene sine opp mot egne erfaringsdatabaser, som for eksempel Microsoft TechNet, og tillater at du selv søker i denne. Noen leverandører krever at du er registrert kunde før du får full tilgang til en slik database.

Andre supportsider

I tillegg til produsentenes nettsider finnes det også en lang rekke nettsider og forum som er dedikert spesielle programmer, systemer eller brukerstøtte generelt. Kvaliteten på slike forum er imidlertid svært variable – noen er glimrende, mens andre i praksis er verdiløse. Som IKT-servicemedarbeider lønner det seg å bygge opp en liste over gode supportsider som du av erfaring vet blir oppdatert regelmessig, og som har et innhold som er til å stole på.

Tech Support Forum, Tech Support GuyCyber Tech Help og den norske Hardware.no er noen eksempler på kjente uavhengige supportsider som har svar på det meste.

Forfatter: Jason Lee

Søkemotorer

Søkemotorer som Google er ofte et godt alternativ for å finne informasjon om spesifikke feilmeldinger, filer og lignende. Men det kan være stor usikkerhet forbundet med kvaliteten på den informasjonen du finner. Når du sliter med sporadiske feil eller ikke kan lokalisere en feil til en bestemt maskindel eller et bestemt program, kan søkemotorer ofte være til god hjelp. Om ikke annet kan resultatene fortelle deg om det er andre som sliter med den samme feilen.

> De fleste problemer som oppstår, er allerede kjent av enten produsenten eller andre brukere.

Feilsøking med søkemotor

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Feilsøking med søkemotor (107707)

Søkemotorer som Google er et godt alternativ for å finne informasjon om spesifikke feilmeldinger, filer, tjenester og prosesser.

Søke etter feilmeldinger med Google

Når du bruker Google, kan du sette **anførselstegn** («…», eller "…") rundt ordene du søker på, slik at Google bare søker etter sider som inneholder det nøyaktige uttrykket. Hvis du søker uten anførselstegn, får du opp alle sider som inneholder en hvilken som helst kombinasjon av ordene.

Hvis du søker på teksten i en feilmelding og setter den i anførselstegn, er det stor sannsynlighet for at du vil få resultater fra forum der andre har spurt om nøyaktig den samme feilmeldingen, og svarene de har fått, vil ofte også være løsningen på ditt problem.

Glem bare ikke at du også må være kritisk til kvaliteten på løsningene. Du bør forsøke å forsikre deg om at forslagene til løsning faktisk løste problemet for den som spurte, og at løsningene gjelder den samme programversjonen eller maskinen som du har problemer med.

Se også på hvor gamle løsningene er, og om det virker som de som har svart, har greie på det de skriver om, eller om de bare gjetter.

Tips når du skal søke etter feilmeldinger

Det er vanligvis ikke mulig å merke tekst i en meldingsboks slik at du kan kopiere og lime den inn i for eksempel Google, men det er mulig å kopiere hele innholdet av meldingen til en tekstfil. Klikk hvor som helst i meldingen unntatt på knappene, og trykk på Ctrl-C. Åpne et nytt tekstdokument og trykk på Ctrl-V. Alt innholdet i meldingen blir kopiert inn i dokumentet som tekst.

1. Klikk på meldingen og trykk Ctrl-C.

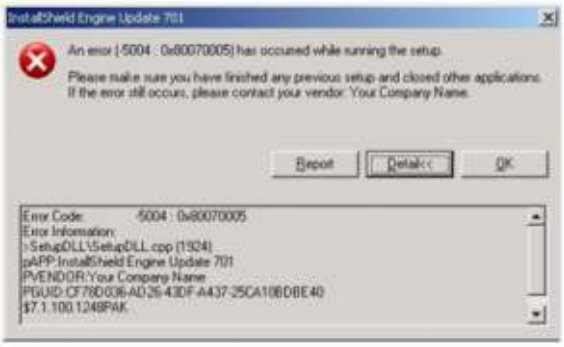
Opphavsmann: Microsoft

2 . Åpne et tekstdokument og trykk på Ctrl-V. Innholdet i meldingen blir limt inn som vanlig tekst.

Opphavsmann: Microsoft

Dette er nyttig både når du skal dokumentere problemer, og når feilmeldingen inneholder lange feilkoder som du skal søke etter i Google.

Noen feilmeldinger har også utvidet informasjon som ikke vises i feilmeldingsvinduet, men som blir tatt med når du kopierer meldingsinnholdet på denne måten.



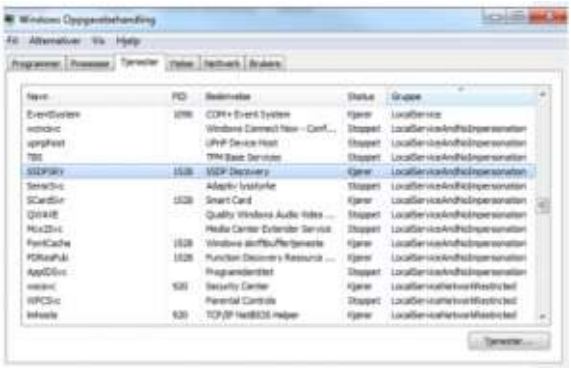
Eksempel på feilmelding med lange feilkoder.

Opphavsmann: Microsoft

Søke etter Windows-prosesser og -tjenester

Google er også godt egnet for å finne informasjon om tjenester (services) eller prosesser som kjører på maskinen.

Illustrasjonen under viser et utsnitt av tjenester i Windows oppgavebehandling. Anta at du lurer på hva tjenesten SSDPSRV gjør, og om den skaper noen problemer.



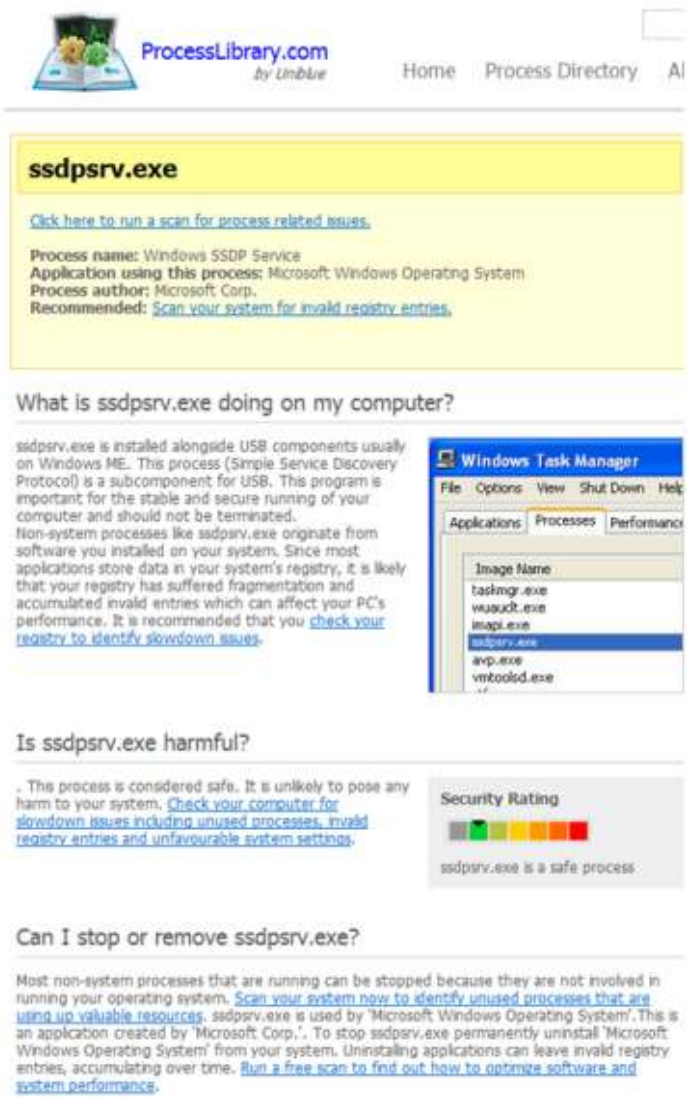
Opphavsmann: Microsoft

Åpne Google og søk på SSDPSRV service.

Søk i Google på SSDPSRV service.

Opphavsmann: Google

Du får resultater fra en rekke nettsider med oversikt over alle typer tjenester og prosesser som finnes i Windows. For eksempel ProcessLibrary.com som forteller at SSDPSRV er en protokoll for kommunikasjon med USB-enheter, at tjenesten ikke er skadelig, og at den bør kjøre. (Se illustrasjon under.)



Søk i Google på SSDPSRV service. Treff hos ProcessLibrary.

Opphavsmann: Microsoft

Søke etter filtyper

På samme måte som for prosesser og tjenester er Google også godt egnet for å finne informasjon om ukjente filer og filtyper.

Anta at du finner en fil med etternavnet .CBZ og lurer på hva slags fil det er, og hvilket program du kan åpne den med.

Ved å søke på CBZ file i Google vil du få nettsider med oversikt over ulike filtyper. For eksempel FileInfo.com. (Se illustrasjon under.)

Søk på CBZ file i Google.

Opphavsmann: Arne Jansen

Informasjon på egne nettsider – Ofte stilte spørsmål

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Informasjon på egne nettsider – ofte stilte spørsmål (107709)

Det kan være fornuftig å lage en nettside med svar på spørsmål som du får ofte. En slik side kalles for en OSS (Ofte Stilte Spørsmål) eller FAQ (Frequently Asked Questions) på engelsk.

Avhengig av innhold kan en OSS (FAQ) enten være intern for virksomhetens brukere på for eksempel et intranett, eller den kan være åpen for virksomhetens kunder på Internett.

En god side med svar på vanlige spørsmål avlaster brukerstøtte, reduserer kostnadene og er praktisk for brukerne siden de slipper å kontakte noen for å få hjelp.

Når du skal lage en OSS må **brukervennlighet** være første prioritet, og det er noen «regler» du bør følge.

Svar på reelle spørsmål

Det er viktig at spørsmålene er reelle. Ikke legg til spørsmål som du tror du vil få i framtiden, eller annen informasjon som du synes bør være med. Husk også at en OSS må oppdateres regelmessig. Start derfor med de spørsmålene du faktisk får, og legg heller til nye etter hvert som de dukker opp. Hvis ingen stiller et bestemt spørsmål, skal det heller ikke være med i en OSS.

Hvis du skal lage en OSS for virksomhetens kunder, kan du også be andre i virksomheten om å samle inn spørsmål for deg. Presiser at du bare vil ha reelle spørsmål.

Del spørsmålene inn i kategorier

En OSS med mange spørsmål bør deles inn i kategorier eller tema slik at brukerne slipper å bla seg gjennom alle spørsmålene for å finne det svaret de leter etter. Men husk på at mange kategorier kan skape usikkerhet om hvor et spørsmål er besvart. En løsning kan være å lage kategorier med undertema.

Skriv i et tydelig «spørsmål–svar» format

En OSS skal bare bestå av spørsmål med svar, og det må være enkelt å se hva som er spørsmål, og hva som er svar, slik at det er mulig å skumlese spørsmålslisten.

Spørsmål og svar kan for eksempel ha forskjellig skrifttype, skriftstørrelse eller farge, eller svaret kan ha et ekstra innrykk sammenlignet med spørsmålet. Andre løsninger er å lage spørsmålslister med lenker til svarene eller svar som ikke vises før man klikker på spørsmålet. (Se illustrasjonen.)

Skriv fullstendige spørsmål

Det må være mulig å forstå hvert spørsmål og svar uavhengig av andre. Derfor bør du skrive fullstendige spørsmål selv om det betyr at spørsmålene blir litt lengre, og at du av og til må gjenta de samme begrepene.

Eksempel på inndeling i tema i Medietilsynets OSS. Opphavsmann: Medietilsynet

Eksempel på kategorier med undertema på Samordnaopptak.no. Opphavsmann: Samordnaopptak

Når spørsmålene er fullstendige, kan de skrives ut, kopieres eller flyttes uten at meningen blir borte. Fullstendige spørsmål gir også bedre resultater hvis noen forsøker å finne svar ved å bruke Google eller en annen søkeside.

I eksemplet under ser du noen ofte stilte spørsmål om energimerking av boliger. De to første spørsmålene er gode, mens de tre neste ikke er fullstendige.

- I stedet for «Hva er poenget med energimerking?» burde det stått «Hva er poenget med energimerking av bolig?».
- I stedet for «Må jeg gjøre det selv?» burde det stått «Må jeg energimerke boligen min selv?».
- I stedet for «Er det vanskelig?» burde det stått «Er det vanskelig å energimerke en bolig?».

I den neste illustrasjonen er spørsmål 5 og tilhørende svar kopiert ut. Det er ikke lett å forstå hva svaret handler om, når spørsmålet ikke er fullstendig.

Eksempel på OSS hos Udir.no, der svaret vises når man klikker på spørsmålet. Legg merke til at spørsmål og svar også er formatert forskjellig.
Opphavsmann: udir.no

Skriv korte svar

En OSS skal gi raskt svar på grunnleggende spørsmål eller problemer og er ikke ment å være en håndbok. Hvis et spørsmål krever et langt svar, bør det heller lenkes til en egen side eller et dokument med mer informasjon som kan lastes ned.

Opphavsmann: NKI Forlaget

Gi brukerne informasjon om hvor de kan få mer hjelp

Hvis brukeren ikke finner svar på spørsmålet sitt i OSS eller fortsatt er usikker på hva han skal gjøre, må det finnes en mulighet for å få mer hjelp. Sammen med OSS-en bør det derfor stå kontaktinformasjon til hvor brukeren kan henvende seg direkte, eller det bør finnes et kontaktskjema som brukeren kan fylle ut.

Lenke:

Designing Effective FAQ Pages

Windows hjelpfunksjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Windows hjelp-funksjon (107716)

De fleste programmer har en innebygget hjelp-funksjon med svar på vanlige brukerspørsmål.

I Windows finner du hjelp-funksjonen i startmenyen under menyvalget «Hjelp og støtte».

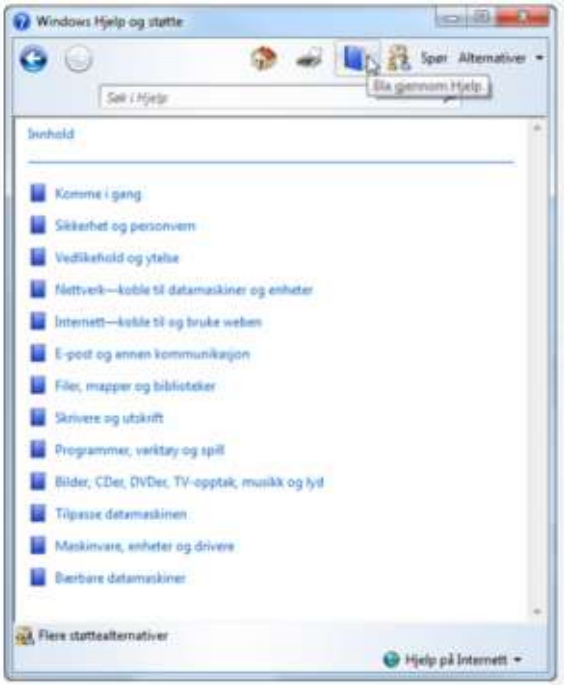
Windows Hjelp og støtte.
Opphavsmann: Microsoft

I søkefeltet øverst kan du skrive inn hva du trenger hjelp til (se figuren under).

Windows Hjelp og støtte søkeresultat.

Opphavsmann: Microsoft

Hvis du ikke finner det du leter etter i søkeresultatet, kan du også bla deg gjennom hjelpetekstene fra menyen (se figuren under).



Windows Hjelp og støtte meny.

Opphavsmann: Microsoft

Hvis informasjonen du trenger, ikke finnes i Windows Hjelp, kan du forsøke Microsofts Windows Hjelp og veiledning på Internett. Her finner du også veiledningsvideoer i tillegg til vanlige hjelpetekster.

Lenke: Using Windows Help & How To

Windows feilsøkere

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Windows feilsøkere (107719)

I tillegg til vanlige hjelp-funksjoner har Windows også innebygde feilsøkingsprogrammer.

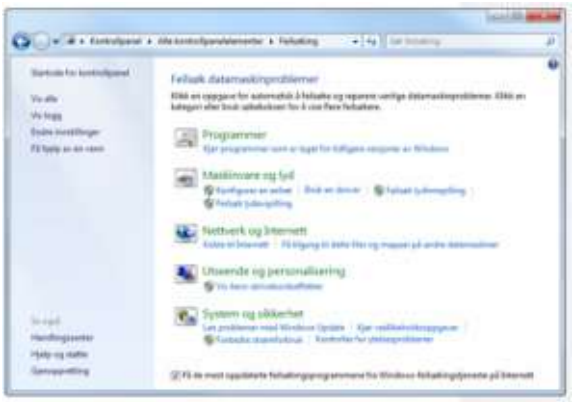
Feilsøkingsprogrammene leder brukeren steg for steg gjennom feilsøkingsprosessen. Det er bare de vanligste og enkleste problemene som kan løses på denne måten, men det kan være en god start for brukerne.

For å vise feilsøkingsprogrammene klikker du startknappen og åpner kontrollpanelet. Velg deretter «Finn og løs problemer» i kategorien «System og sikkerhet» (se figuren under).

Windows kontrollpanel.

Opphavsmann: Microsoft

Fra menyen velger du den oppgaven du trenger hjelp med (se figuren under). Programmet starter og leder deg gjennom feilsøkingsprosessen.



Windows feilsøkingsprogrammer.

Opphavsmann: Microsoft

Lenke: Løse vanlige problemer ved hjelp av feilsøkere.

Windows fjernhjelp

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Windows fjernhjelp (107721)

Noen ganger er det behov for å vise brukeren hvordan et problem eller en oppgave løses, men det er ikke alltid mulig å oppsøke brukeren. For å løse dette har Windows en innebygd funksjon for fjernhjelp.

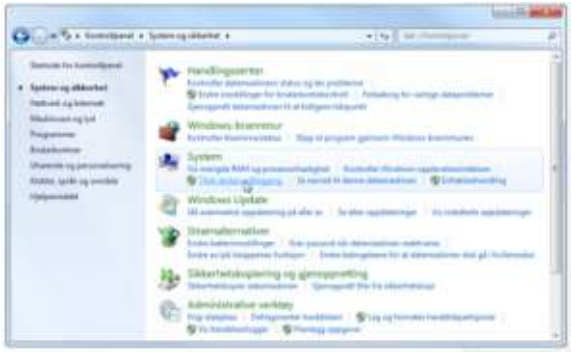
Stadig flere bruker bærbare maskiner og har behov for hjelp mens de for eksempel er på reise eller jobber hjemmefra. Windows fjernhjelp gir brukeren mulighet for å gi deg fjerntilgang til pc-en sin via Internett slik at du kan fjernstyre den og løse et problem eller vise hvordan en oppgave skal gjøres.

Selve oppkoblingen er passordbeskyttet og kryptert slik at det ikke skal være mulig for uvedkommende å koble seg til pc-en.

For å sette opp en fjernhjelpoppkobling må den som trenger hjelp, først tillate fjernhjelptilkoblinger til maskinen sin, og deretter må vedkommende sende deg en invitasjon om fjernhjelp.

Tillate fjernhjelptilkobling

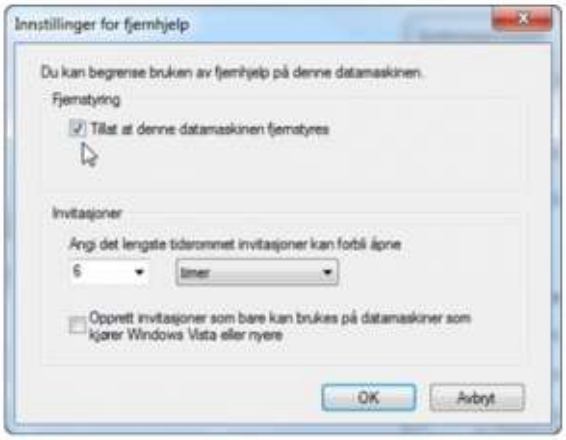
1. Klikk på Start-knappen, åpne kontrollpanelet og velg «System og sikkerhet».
2. Velg «Tillat ekstern pålogging» fra «System og sikkerhet» (se figuren under).



Windows System og sikkerhet.

Opphavsmann: Microsoft

3. Dialogboksen for Systemegenskaper åpnes. Velg fanen Eksternt og klikk på knappen Avansert.
4. Merk boksen for «Tillat at denne datamaskinen fjernstyres» (se figuren under).



Windows Innstillinger for fjernhjelp.

Opphavsmann: Microsoft

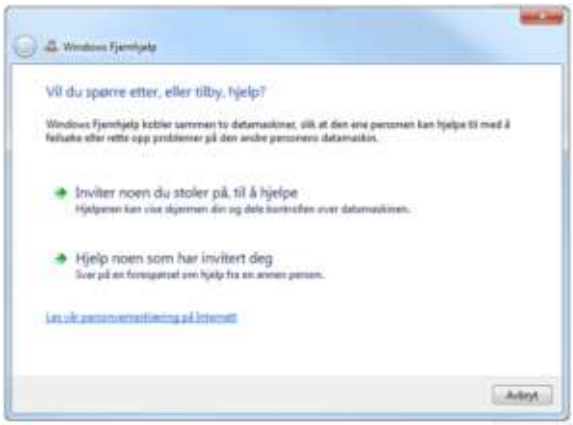
Maskinen er nå klar for å kunne motta fjernhjelp.

Starte fjernhjelpoppkoblingen

Det finnes to måter å sette opp en fjernhjelpoppkobling på.

- Bruk «Enkel tilkobling» hvis begge datamaskinene bruker Windows 7 eller nyere.
- Lag en invitasjonsfil hvis den ene datamaskinen bruker en annen Windows-versjon eller enkel tilkobling ikke er tilgjengelig.

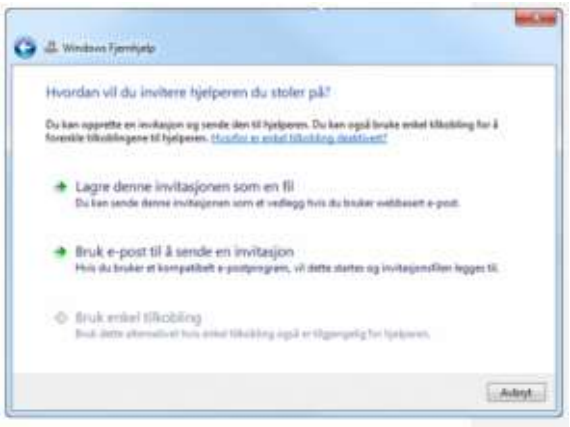
1. Start Windows fjernhjelp fra mappen Vedlikehold i Start-menyen eller ved å klikke på «Flere støttealternativer» nederst i vinduet for Windows Hjelp og støtte.
2. Klikk «Inviter noen du stoler på, til å hjelpe» (se figuren under).



Windows Fjernhjelp.

Opphavsmann: Microsoft

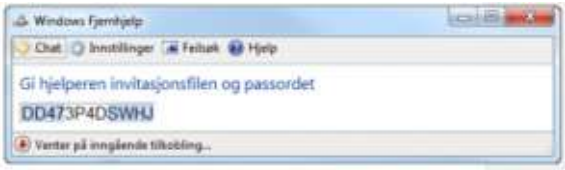
3. Lag en invitasjonsfil eller bruk en enkel oppkobling, og merk at alternativet for enkel oppkobling ikke alltid er tilgjengelig (se figuren under).



Windows Fjernhjelp invitasjon.

Opphavsmann: Microsoft

4. Hvis oppkoblingen skal gjøres med invitasjonsfil, må brukeren sende deg denne filen først, for eksempel som et vedlegg i en e-post. I tillegg må du få passordet som Windows har generert spesielt for fjernhjelpoppkoblingen. Passordet vises i et eget vindu på brukerens maskin (se figuren under).



Windows Fjernhjelp passordgenerator.

Opphavsmann: Microsoft

Av sikkerhetshensyn bør ikke invitasjonsfilen og passordet sendes sammen. Hvis invitasjonen sendes på e-post, bør du få passordet på telefon eller i en egen e-postmelding.

5. Når du har mottatt invitasjonsfilen og passordet, starter du Windows fjernhjelp på maskinen din og velger «Hjelp noen som har invitert deg».
6. Velg «Bruk invitasjonsfil» og tast inn passordet.
7. På brukerens maskin vises en dialogboks med spørsmål om å akseptere tilkoblingen. Brukeren må svare Ja på dette.
8. Nå vises skjermbildet på brukerens maskin på din maskin i fjernhjelpvinduet. Klikk på valget «Be om kontroll» øverst til venstre i vinduet.
9. Brukeren får spørsmål om han vil la deg få kontroll med maskinen (se figuren under).

Windows fjernhjelp bekreftelse på deling av kontroll.

Opphavsmann: Microsoft

10. Når brukeren har svart bekreftende, kan du styre brukerens mus og tastatur. På brukerens skjerm vises en meny med mulighet for å stanse eller pause delingen. I tillegg er det en chat-funksjon som kan brukes til å kommunisere mens du løser problemet eller viser brukeren hva han skal gjøre (se figuren under).

Windows fjernhjelp meny på brukerens maskin.

Opphavsmann: Microsoft

Lenke: Video – Using Windows Remote Assistance to get help with your computer.

Oppgave

Samarbeid med en annen i klassen eller noen du kjenner, og opprett en Windows fjernhjelptilkobling. Bytt på hvem som er hjelper, og hvem som blir hjulpet.

Dokumentasjon og tilgjengeliggjøring

Hvorfor du må dokumentere

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hvorfor du må dokumentere (109214)

Å dokumentere er en del av de arbeidsoppgavene til IKT-servicemedarbeideren som oftest blir oversett og undervurdert.

Å dokumentere de feilene og problemene som oppstår, og hvordan de ble løst, er en svært viktig del av IKT-support og drift. Når du dokumenterer systematisk, bygger du opp kunnskap og verdifull informasjon om de systemkombinasjonene virksomheten har, og de spesielle feilene og problemene som kan oppstå.

Du tenker kanskje at du vil huske hvordan et bestemt problem ble løst, men når et tidligere problem dukker opp igjen senere, har man som regel glemt detaljene. Du kommer sikkert ikke til å være i samme jobb for all fremtid heller, og den erfaringen du bygger opp og dokumenterer, er derfor uvurderlig for den som skal overta jobben din. Når du dokumenterer, gjør du det altså både for din egen skyld og for andres.

Tenk også på at når du dokumenterer løsninger på problemer, bygger du opp kunnskap som du senere kan dele med andre i et kunnskapsnettverk.

Noen unngår til og med bevisst å dokumentere løsninger på problemer fordi de gjerne vil gjøre seg uunnværlige. Tanken er at kunnskap er makt, og så lenge man er den eneste som er i stand til å løse problemene, er jobben trygg. Det burde være opplagt at dette ikke er en strategi du bør satse på. Det er ved å dokumentere at du beviser din verdi som en dyktig IKT-servicemedarbeider.

Opphavsmann: Knut Høihjelle

Det er ved å dokumentere at du beviser din verdi som en dyktig IKT-servicemedarbeider.

Dokumentere løsninger på problemer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Dokumentere løsninger på problemer (109215)

Det viktigste er ikke hvordan du dokumenterer løsninger på problemer, men at du forstår nødvendigheten av å gjøre det og faktisk gjør det.

I forbindelse med helpdesk lærte du at det er viktig å registrere alle henvendelser og løsninger i en supportdatabase slik at de som betjener helpdesken, raskt kan finne løsningen på kjente problemer. I kompetansemålet om bruk av hjelpfunksjoner og kunnskapsdatabaser var erfaringsdatabaser (egne og andres erfaringer) en viktig kilde til informasjon.

Slike informasjonsdatabaser har to kjennetegn:

- De er strukturerte og løsningsorienterte.
- De blir ajourført fortløpende.

Med «strukturert og løsningsorientert» mener vi at dokumentasjonen følger en fastsatt mal og hvert problem har sin egen oppføring som bare inneholder informasjon om hvordan det bestemte problemet kan løses.

Det finnes ikke noen fasit for hvordan en slik mal bør se ut, men det er hensiktsmessig å dele informasjonen inn i tre deler:

1. beskrivelse av problemet
2. årsaken til problemet
3. løsningen på problemet

Beskrivelsen av problemet forklarer kort hvordan problemet arter seg. For eksempel hva som skjer eller ikke skjer, hva som vises på skjermen, eller andre konsekvenser av problemet.

Årsaken er hva som forårsaker eller utløser problemet. Det kan være brukerfeil, en programfeil, defekt maskinvare og så videre.

Løsningen er beskrivelsen av hva som må gjøres for å ordne feilen.

Med «ajourføres fortløpende» mener vi at informasjon om problemet legges inn så snart som mulig. I forbindelse med helpdesker som har telefonsupport eller fjernsupport, er det ikke uvanlig at supportmedarbeideren dokumenterer mens han snakker med brukeren.

Helpdesken kan ha god nytte av grundig dokumentasjon.
Fotograf: Corbis

Ta notater fortløpende mens du løser brukerproblemer, så går det raskt å gjøre dem tilgjengelig for deg selv og andre etterpå.
Fotograf: Berit Roald

Venn deg til å ta notater med en gang slik at du ikke glemmer viktige detaljer.

Det er selvsagt ikke alltid mulig å skrive ned alt mens du jobber med å løse feilen, men du bør venne deg til å ta notater så snart som mulig slik at du ikke glemmer viktige detaljer. Du kan for eksempel bruke en mobiltelefon eller et nettbrett til å notere på når du er hos brukere, slik at du kan overføre informasjonen direkte til en database senere.

Det viktigste er ikke hvordan du dokumenterer løsninger på problemer, men at du forstår nødvendigheten av å gjøre det og faktisk gjør det.

Dokumentere rutiner

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Dokumentere rutiner (109219)

I tillegg til å dokumentere løsninger på problemer er det viktig å dokumentere rutiner.

En rutine kan defineres som

«*et sett med oppgaver som skal gjøres på samme måte og i samme rekkefølge hver gang de utføres*».

I motsetning til løsninger på problemer, som kanskje bare dukker opp én gang, er rutiner oppgaver som skal utføres regelmessig (for eksempel sikkerhetskopiering), eller oppgaver som skal utføres på en bestemt måte når de må gjøres (for eksempel tilbakekopiering av en sikkerhetskopi).

Man må dokumentere rutiner av to grunner:

- for at oppgaven skal bli gjort
- for at oppgaven skal bli gjort riktig

Å lage rutiner er en måte å sikre at oppgaver blir gjort på, og alle rutinebeskrivelser skal si noe om hvem som er ansvarlig, og når eller i hvilken sammenheng rutinen skal utføres. Det må ikke nødvendigvis være en bestemt dato eller et bestemt tidsintervall – rutiner kan også knyttes opp til andre oppgaver eller bestemte hendelser. For eksempel vil en rutine for tilbakekopiering av en sikkerhetskopi bare være aktuell når data har gått tapt.

Å dokumentere rutiner på en god måte kan være omstendelig, men samtidig tvinges du til å gjennomgå alle de arbeidsoppgavene rutinen innebærer, på en systematisk måte. Den beste måten å dokumentere en rutine på, er å skrive ned hva du gjør, mens du utfører oppgaven.

Når du dokumenterer en rutine, må du passe på at informasjonen er så komplett at andre kan følge den steg for steg senere og oppnå riktig resultat. Rutinebeskrivelser kan derfor bli svært detaljerte, og noen ganger er det nødvendig å dele opp en større rutine i flere delrutiner.

Rutinebeskrivelsen må også inneholde informasjon om hva som eventuelt må gjøres før eller etter selve oppgaven, og annet som er nødvendig for å få gjort den. For eksempel må en rutine for tilbakekopiering av sikkerhetskopi inneholde informasjon om hvor

Husk gode rutiner for sikkerhetskopiering!

Fotograf: Simon Chavez

Lenke

Guide til god driftsdokumentasjon

(Fra Auduns IT-weblogg)

Rutine for sikkerhetskopiering av server / fil
http://ndla.no/nb/node/109218

finner du et eksempel på en rutine for sikkerhetskopiering av server.

Den beste måten å dokumentere en rutine på er skrive ned hva du gjør, mens du utfører oppgaven.

sikkerhetskopiene oppbevares.

Alle rutiner bør inneholde informasjon om

- hva rutinen gjelder
- når den skal utføres
- hvem som skal utføre rutinen
- hvem som er ansvarlig for at rutinen utføres (og hvem man skal rapportere til)
- hva som kreves for å utføre rutinen (for eksempel utstyr, programvare, tilganger og så videre)
- hvem som har skrevet rutinen
- når rutinen er skrevet eller sist oppdatert
- om rutinen er en delrutine som inngår i en større rutine
- steg-for-steg-beskrivelser av hva som skal gjøres

Steg-for-steg-beskrivelser kalles også for prosedyrer. Du lærer mer om hvordan du skal skrive prosedyrer litt senere.

Skrive brukerdokumentasjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Skrive brukerdokumentasjon (109223)

De aller fleste som jobber med IKT, vil på et eller annet tidspunkt få behov for å skrive informasjon eller dokumentasjon som skal leses og forstås av brukere.

Det kan være en utfordring – det er ofte vanskeligere enn man tror – å skrive god brukerdokumentasjon. Sjansen for et godt resultat øker imidlertid betraktelig hvis du stiller deg selv noen enkle spørsmål før du begynner å skrive:

- Hvem skriver jeg for?
- Hvilket kunnskapsnivå har brukeren?
- Hvorfor leser brukeren dokumentasjonen?
- Når og hvor leser brukeren dokumentasjonen?
- Hva vil jeg oppnå med dokumentasjonen?
- Hvilket detaljnivå er nødvendig?
- Kan illustrasjoner eller video være til noen hjelp?

Ved å besvare disse spørsmålene blir du bevisst på hvem du skriver for, og hva dokumentasjonen må inneholde for at den skal bli forståelig og nyttig for den som skal lese. I tillegg unngår du å ta med informasjon som er unødvendig, eller som kanskje ikke blir forstått eller lest i det hele tatt.

I noen tilfeller vil brukeren også være usikker på om den informasjonen han har funnet frem til, er den riktige, om den er ment for ham, og om han behøver og lese den. God brukerdokumentasjon tar hensyn til dette og opplyser med en gang leseren hvem den er beregnet for, og hva han kan forvente å finne informasjon om. (Se eksempel i figuren under.)

Brukerdokumentasjon for SuperDuperApp 2.0

Beregnet for: Alle nye brukere av SuperDuperApp 2.0

Forklarer: Grunnleggende rutiner. Innlogging, registrering og utskrift.

Hensikt: Hjelpe nye brukere med å komme i gang med SuperDuperApp 2.0 og besvare vanlige spørsmål i forbindelse med oppstart.

INNHOLD

Hvordan starte SuperDuperApp 2.0	Side 2
Innlogging	Side 3
Registrere en ny kunde	Side 4
Registrere en bestilling	Side 5
Skrive ut en bestilling	Side 7

Eksempel på innledning til brukerdokumentasjon.

Opphavsmann: Arne Jansen

Ved å spesifisere hvem dokumentet er beregnet for, noen stikkord om hva det inneholder, og hvorfor du har skrevet det, får brukeren med en gang mulighet til å avgjøre om dette er noe han bør lese. Videre bør dokumentet ha en innholdsfortegnelse som gjør at det er enkelt å finne frem.

Legg merke til at det å kunne besvare de spørsmålene vi listet opp innledningsvis, er utgangspunktet både for innledningen til dokumentasjonen og hvilket innhold som skal være med.

> God brukerdokumentasjon opplyser med en gang leseren hvem den er beregnet for, og hva han kan forvente å finne informasjon om.

Skrivetips

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Skrivetips (109224)

Ikke alle er forfattere – og det er heller ikke nødvendig for å skrive brukerdokumentasjon. Det vesentlige er at informasjonen er lettest, og at den blir forstått.

Bruk enkelt språk og korte setninger

Korte setninger er lettere å lese og lettere å forstå. Unngå også å bruke mange lange og vanskelige ord. Det er ikke alle som leser like godt.

Faguttrykk kan by på spesielle problemer fordi du ikke kan være sikker på at brukeren forstår dem. Generelt bør du forsøke å unngå faguttrykk, men i noen tilfeller er det uunngåelig. Er du usikker på om brukeren kommer til å forstå et uttrykk, bør du forklare det den første gangen du bruker det.

Det som er opplagt for deg, er ikke alltid like opplagt for andre

Vær bevisst på hvem du skriver for, og hvilket kunnskapsnivå brukeren har. Du kjenner ditt eget fagfelt godt, og det er derfor fort gjort å forenkle stoffet slik at det blir uforståelig for brukeren. Samtidig må du selvsagt ikke undervurdere brukerens kunnskapsnivå og plage ham med for mange unødvendige detaljer heller.

Vær konsekvent

Ofte finnes det flere uttrykk og skrivemåter som i praksis betyr det samme, men dette kan virke forvirrende på brukeren. Hvis du har begynt å skrive for eksempel *skriver*, bør du være konsekvent og ikke skrive *printer* senere.

Bruk stavekontrollen

Det burde være unødvendig å si det, men stavefeil er unødvendig og får dokumentasjonen til å virke uprofesjonell. Hvis du ikke stoler på stavekontrollen, kan du la noen andre lese gjennom og rette eventuelle skrivefeil for deg.

Hvis det er vanskelig å forklare, vis det i stedet

Skrivefeil kan være morsomme og sjarmerende i visse sammenhenger, men i brukerdokumentasjon bør du passe på å unngå stavefeil.
Fotograf: Berit Keilen

Det vesentlige er at informasjonen er lettest, og at den blir forstått.

Her ser du et eksempel på hvordan skjermdumper og tekst kan spille sammen og forenkle forståelsen for leseren.

Her kan du finne et eksempel på en enkel brukerveiledning i videoformat: Skifte blekk i printeren

Bilder av programvinduer sammen med tekst gjør det enklere for brukeren å se hvor han skal klikke, og hvordan skjermen hans skal se ut underveis. En annen mulighet er å bruke et verktøy for å spille inn det som skjer på skjermen mens du utfører en oppgave, og deretter lagre det som en video.

Bruk av bilder og video gjør at du kan skrive mindre, og du kan bruke bilder til annen dokumentasjon også. Det er for eksempel enklere å ta noen bilder eller lage en video av hvordan man skal skifte blekkpatron i en skriver, enn å forklare hele prosessen med ord. Dette kan du se mange eksempler av på YouTube, der både produsenter og brukere har lagt ut videoer med brukerveiledninger, tips og demonstrasjoner.

Skrive for skjerm

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Skrive for skjerm (109228)

Stadig mer informasjon publiseres som nettsider på Internett eller på et intranett. Å skrive informasjon som skal leses på skjerm, krever at du er oppmerksom på at de fleste leser tekst på skjerm på en litt annen måte enn når de leser på papir.

De fleste har en tendens til å «skumme» en tekst på skjerm og plukke ut det som ser interessant ut, i stedet for å lese teksten sammenhengene slik vi vanligvis gjør på papir. Vi leser i større grad bruddstykker av teksten og hopper mer frem og tilbake.

En tekst som skal leses på skjerm, bør derfor være skrevet slik at den egner seg for slik «skumming». Det oppnår du ved å huske på følgende:

Uthev nøkkelord

Vi stopper opp ved det som **skiller seg ut**, som for eksempel de tre ordene du nettopp leste. Ved å markere ord og begreper som er særlig viktige i teksten, kan du lede brukerens oppmerksomhet dit. Man kan utheve på vanlig måte, for eksempel ved å streke under eller bruke farger.

Bruk meningsfulle avsnittsoverskrifter

Vi leser nesten alltid avsnittsoverskriftene, så det er viktig at de er så meningsfulle som mulig. Det vil si, de bør beskrive innholdet i det avsnittet som følger. Unngå morsomme eller «smarte» overskrifter i brukerdokumentasjonen.

Bruk punktlister

Punktlister er raske å skumlese, så de blir derfor nesten alltid lest.

Ha kun ett poeng per avsnitt

Når du har flere poenger du vil formidle, bør du skille dem godt slik at hvert poeng får sitt eget avsnitt.

Start med konklusjonen

Fotograf: Corbis

En godt utformet tekst gjør det enkelt for brukeren å lese.
Fotograf: Ingar Haug Steinholt

Husk

- Start med konklusjonen.
- Uthev nøkkelord.
- Lag gode overskrifter.
- Bruk punktlister.
- Ha ett poeng per avsnitt.

- Bruk få ord.

Innledningen eller det første avsnittet blir nesten alltid lest, og det vesentlige bør derfor stå der, slik at det er større sjanse for at brukeren får det med seg. Tenk på hvordan avisartikler er bygget opp. Hovedpoenget kommer i overskriften og ingressen, deretter følger detaljene i selve teksten.

Bruk færre ord

Som hovedregel bør du forsøke å bruke færre ord når du skriver for skjerm enn for papir. De fleste setningene kan gjøres kortere uten at meningen forsvinner. Se på eksempelet under. Alle de fire setningene sier egentlig det samme, men den første har nesten fire ganger så mange ord som den siste.

- Vi forstår innholdet i en tekst selv om den ikke har så mange ord.
- Vi forstår innholdet i en tekst som har få ord.
- Vi forstår innholdet i en kort tekst.
- Vi forstår kort tekst.

Skrive prosedyrer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Skrive prosedyrer (109233)

Brukerinformasjon skal ofte inneholde prosedyrer som brukeren kan følge steg for steg for å få utført en bestemt oppgave.

Prosedyrer er ofte en viktig del av rutiner eller brukerdokumentasjon. Det finnes ikke noen standard for hvordan man skal skrive prosedyrer, men det er noen prinsipper du bør følge.

Under ser du et eksempel på en prosedyre for hvordan man slår på visningen av skjulte filer og mapper i Windows utforsker.

1. Åpne **Windows Utforsker** (*Startknappen – Datamaskin*).
2. Velg menyen **Organiser** og **Mappe og søkealternativer**.
   Dialogboksen Mappealternativer vises.
3. Velg fanen **Vis**.
4. Velg rullefeltet **Avanserte innstillinger**, rull ned til **Skjulte filer og mapper**.
5. Klikk på radioknappen **Vis skjulte filer, mapper og stasjoner**.
6. Klikk **OK**.

Eksempelet viser de viktigste prinsippene for å skrive prosedyrer.

De valgene brukeren skal gjøre, er tydelig markert (uthevet)

Når man uthever de valgene som skal utføres i hvert steg, kan hele prosedyren sammenfattes ved å bare bruke de uthevede ordene:

- **Windows Utforsker**
- **Organiser – Mappe og søkealternativer**
- **Vis**
- **Avanserte innstillinger – Skjulte filer og mapper**
- **Vis skjulte filer, mapper og stasjoner**
- **OK**

Det gjør at erfarne brukere kan jobbe seg gjennom en prosedyre uten å måtte lese all teksten. Det er også tidsbesparende hvis man må utføre en prosedyre flere ganger.

Tilleggsinformasjon og kommentarer er satt i kursiv

Det er ikke vesentlig hvilken løsning du velger – så lenge du bruker den konsekvent.

Når du er på arbeid som IKT-servicemedarbeider, kan det være til stor hjelp å ha gode prosedyrer du kan følge.
Fotograf: RAHEB HOMAVANDI

Som bruker kan du også ha stor glede av gode prosedyrebeskrivelser. Kanskje du har erfaring med å bruke prosedyrer når du har løst problemer på skolen eller hjemme?
Fotograf: Bjørn Aslaksen

Vi antar at de fleste vet hvordan de skal åpne Windows Utforsker i linje 1, men for de som eventuelt er usikre, er veien vist i kursiv parentesen (*Startknappen – Datamaskin*). I prosedyrer kan vi bruke kursiv tekst til tilleggsinformasjon og kommentarer.

Alle stegene i prosedyren er nummerert

Nummerering gir bedre oversikt og gjør det enklere å følge en prosedyre. Det er også lettere å referere til et nummer i en prosedyre ved for eksempel telefonsupport.

Alle stegene står i den rekkefølgen de skal utføres

Det er viktig at alle steg står i den rekkefølgen de skal utføres, både linje for linje og innbyrdes på hver linje. De to setningene under beskriver det samme steget, men bare den siste er riktig når du skal skrive en prosedyre.

- Velg **Mappe og søkealternativer** fra menyen **Organiser**.
- Velg menyen **Organiser** og **Mappe og søkealternativer**.

Den første setningen beskriver ikke valgene i den riktige rekkefølgen, og da blir det vanskeligere å følge prosedyren. Hvis vi forsøker å sammenfatte ved bare å lese de uthevede ordene, blir prosedyren feil.

Prosedyren beskriver resultatet av en handling og det man skal se på skjermen

Når en handling skal medføre at noe skjer, bør resultatet alltid beskrives. I linje 2 får brukeren vite at det skal komme opp en dialogboks med tittelen Mappealternativer når han har valgt Mappe og søkealternativer. Hvis boksen vises, vet han at han kan gå videre til neste punkt. Hvis den ikke vises, vet han at noe er galt, og at han må gå tilbake til forrige punkt i prosedyren.

Vi kunne også ha erstattet beskrivelsen med en illustrasjon som viste dialogboksen. Bruk av illustrasjoner er en effektiv måte å vise brukeren hva han skal se på skjermen sin. Men pass på å ikke overdrive bruken av illustrasjoner og skjermbilder, for det kan gjøre prosedyren uoversiktlig.

Tenk også på at skjermbildene du ser på din maskin, ikke alltid er helt identiske med det brukeren ser på sin maskin. Forskjeller i skjermoppløsning, fargevalg, temaer, programversjoner og så videre kan medføre at det er forskjell på illustrasjonen og det brukeren ser på sin skjerm, og da kan brukeren bli usikker.

Det finnes som sagt ikke noen standard for hvordan man skal skrive en prosedyre. Du vil derfor kunne se mange andre løsninger hvor man bruker utheving, kursiv, understreking eller varierer med skrifttyper. Det er heller ikke så viktig hvilken løsning du velger – så lenge du bruker den konsekvent. Det blir fort forvirrende hvis for eksempel noen menyvalg er uthevet og andre er understreket.

Det er også lurt å unngå å bruke farger for å skille de ulike delene av en prosedyre. Det er nyttig for brukeren å kunne forstå informasjonen også på en sort-hvitt-utskrift.

Distribuere informasjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Distribuere informasjon (109234)

Når man har skrevet brukerinformasjon, må man velge hvordan man skal distribuere den. Det er flere mulige måter å distribuere på, og alle har sine fordeler og ulemper.

De tre mest aktuelle måtene å distribuere informasjon på er papir, e-post eller publisering på nett, for eksempel virksomhetens intranett.

Papir

Å distribuere informasjon på papir er arbeidskrevende og kostbart sammenlignet med alternativene, men vi skal ikke avskrive papir helt likevel. Informasjon som mottas på papir, blir ofte oppfattet som viktigere enn noe som kommer som e-post, og det er derfor større sjanse for at informasjonen blir lest og tatt vare på.

E-post

E-post er en effektiv måte å distribuere informasjon på, men den er ikke alltid like hensiktsmessig. De fleste som arbeider i en virksomhet, mottar et stort antall e-postmeldinger hver dag. Hvis informasjonen ikke er aktuell akkurat når e-postmeldingen leses, er det store muligheter for at den blir arkivert, glemt eller slettet. Det gjør det vanskelig for brukeren å finne informasjonen senere, når han har behov for den.

En mulighet er å sende informasjonen som vedlegg i en e-post. Det øker mulighetene for at den blir tatt vare på, men samtidig krever det en del ekstra arbeid fra brukerens side; vedlegget må lastes ned, åpnes eller eventuelt skrives ut før informasjonen kan leses. E-post bør derfor helst bare benyttes til å distribuere informasjon som skal brukes med en gang.

Publisering på nett

Publisering på nett er ofte den mest effektive måten å distribuere informasjon på. Metoden er kostnadseffektiv og krever som regel lite arbeid hvis virksomheten har en intranettløsning eller tilsvarende informasjonstjeneste. Ulempen er at brukerne selv må oppsøke informasjonen når de trenger den. Hvis de ikke er aktive brukere av informasjonstjenesten, når informasjonen sent eller aldri fram.

Det er fremdeles mulig å sende ut informasjon til kollegaene dine på papir, men vurder når denne løsningen er mest hensiktsmessig.
Fotograf: Lars Bahl

E-post er en effektiv måte å distribuere informasjon på, men innholdet kan lett forsvinne blant mange andre e-poster.
Fotograf: NKI Forlaget

Informasjon som legges på nettsider, bør alltid være i et format som kan skrives ut.

Informasjon som legges ut på nettsider, bør alltid være i et format som kan skrives ut. Dette er spesielt viktig for prosedyrer der brukeren vil ønske å kunne lese instruksjonene samtidig som han utfører dem på maskinen.

Behovet for oppdateringer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Behovet for oppdateringer (109235)

Informasjon må oppdateres eller fjernes når det skjer endringer som gjør at informasjonen ikke lenger er korrekt eller aktuell. Foreldet eller feil informasjon kan i noen tilfeller skape flere problemer enn ingen informasjon i det hele tatt.

I praksis viser det seg at det er langt vanskeligere å holde informasjon oppdatert enn det man i utgangspunktet skulle tro. I de fleste virksomheter trenger man ikke å lete lenge for å finne utdatert informasjon. Bruk av Internett/intranett har heller ikke gjort situasjonen bedre.

Problemet med utdatert informasjon oppstår fordi det ofte finnes en rutine for å dokumentere, men ingen rutine for å oppdatere eller fjerne gammel dokumentasjon. En annen årsak er at ansatte slutter, og at den som overtar, er usikker på om gammel dokumentasjon er utdatert eller ikke. Da føles det ofte tryggere å ikke gjøre noe enn å risikere å fjerne noe som kanskje fortsatt er aktuelt.

Du vil aldri kunne eliminere problemet med utdatert informasjon helt, men her er noen enkle grep som kan hjelpe langt på vei:

- Lag en rutine for regelmessig gjennomgang og oppdatering av informasjon som du er ansvarlig for. En fullstendig gjennomgang for eksempel hvert halvår sikrer at du i det minste får luket ut de fleste gamle dokumentene.
- Dater all informasjon tydelig slik at det er mulig å se hvor gammel den er, og når den sist ble oppdatert. Mange foretrekker å gjøre dette i bunnteksten, men det beste er å skrive det i begynnelsen av dokumentet.
- Sett en «best før»-dato på informasjon som er «ferskvare»; marker den tydelig med en dato som sier når den ikke lenger er aktuell.
- Sørg for at én person i bedriften har ansvaret for å følge opp og oppdatere kritiske rutiner og viktig dokumentasjon.

Foreldet eller feil informasjon kan i noen tilfeller skape flere problemer enn ingen informasjon.

Viktige rutiner - som branninstrukser – må oppdateres straks det skjer endringer. Da er det viktig at én person eller avdeling har ansvar for at dette blir gjort.
Fotograf: NKI Forlaget

Her ser du et eksempel på at artikkelsen på et nettsted er datert med både opprettet dato og endret dato. Dette gjør det enkelt å avgjøre om teksten fremdeles er aktuell eller ikke.

Oppgaver

Rutinebeskrivelse

Forfatter: Arne Jansen, Amendor AS, NKI Forlaget
Rutinebeskrivelse (109221)

Hensikten med denne oppgaven er at du skal få øve på å skrive rutinebeskrivelser. Oppgaven bør gjøres som gruppearbeid.

Anta at du arbeider som IKT-servicemedarbeider i en middels stor virksomhet. Virksomheten har ganske mange ansatte og bruker også en del vikarer i ferier og ved sykemeldinger. Når en ny person blir ansatt, må vedkommende få en brukerkonto i nettverket. For å unngå at denne prosedyren blir tilfeldig, skal du lage en rutine for hvordan dette skal håndteres.

Du må tenke gjennom hvilke personer som må involveres, hvilke standarder som skal følges, hvilken informasjon som må samles inn, hvilken informasjon som må gis ut, hvordan informasjonen skal gis, og så videre.

Her er noen forslag til hva du kan vurdere:

- Hvem er ansvarlig for å gi beskjed om når en ny bruker skal opprettes?
- Hvem bestemmer hvilke tilganger brukeren skal ha?
- Hva skal standarden for brukernavn og passord være?
- Hva skal standarden for e-postadresse være?
- Skal brukeren ha et eget dataområde på serveren?
- Hvem er ansvarlig for å informere brukeren om hvordan han logger seg på?
- Hvem er ansvarlig for at en brukerkonto blir slettet eller deaktivert når en person slutter?
- Hva skal skje med data som ligger på personlig dataområde eller e-post som ligger igjen etter en bruker som slutter?

Listen er ikke komplett, men er ment å gi en idé om hva slags informasjon du kan ta med i rutinen.

Merk at det *ikke* er meningen at du skal skrive noen steg-for-steg-beskrivelser som viser hvordan man oppretter brukere, e-postkontoer eller lignende i denne oppgaven.

Informasjon for skjerm

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Oppgave - Informasjon for skjerm (109231)

Hensikten med denne oppgaven er at du skal få øvelse i å skrive informasjon for skjerm. Du kan gjøre oppgaven individuelt eller sammen med en annen.

Under ser du en tekst som er dårlig formatert og ikke spesielt godt skrevet. Skriv om teksten slik at den blir lettere å forstå – uten at det vesentlige i innholdet forsvinner. Formater den på en slik måte at den er bedre egnet for å lese på skjerm.

Behandling av datamaskiner på arbeidsplassen

For å redusere antallet "unødvendige" support og service henvendelser til it-avdelingen, og forlenge levetiden på bedriftens datautstyr, vil vi at alle ansatte skal merke seg følgende retningslinjer for behandling av datamaskiner på arbeidsplassen.
Alle ansatte skal slå av maskinen og alt tilkoblet utstyr som printere, skannere osv. når de avslutter arbeidet for dagen. Maskinen skal slås av ved å bruke avslutt funksjonen som finnes på startknapp menyen i Windows. Før du slår av maskinen må du avslutte alle programmer og vinduer som er åpne.
Det har vært en del problemer med kabler som enten er blitt ødelagt eller er blitt plassert slik at de har forårsaket uhell. Alle kabler som er tilknyttet datamaskinen må plasseres slik at de ikke kommer i klemme for eksempel mellom vegg og skrivebord eller under maskinen. Kabler må heller ikke ligge løst på gulvet slik at de er i veien for rengjøringspersonellet eller at man risikerer å dra de med seg med stolen eller foten. I et tilfelle gikk en skjerm i gulvet på grunn av dette. Maskinen må ikke plasseres så langt fra uttaket til nettverk at nettverkskabelen blir strammet. Vi har hatt flere tilfeller av at maskiner har mistet kontakten med nettverket på grunn av dette. Lengre kabler er tilgjengelig i it-avdelingen.
Så langt det er mulig bør du unngå å spise når du sitter ved maskinen og brusflasker og kaffekopper må plasseres slik at de ikke risikerer å veltes over tastaturet.

Et eksempel på en tekst som er dårlig formatert og ikke spesielt godt skrevet.

Opphavsmann: Arne Jansen

Skrive brukerinformasjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Skrive brukerinformasjon (109227)

Hensikten med denne oppgaven er at du skal få øve deg på å skrive informasjon for brukere. Oppgaven bør gjøres individuelt.

Tenk deg at du er IKT-servicemedarbeider i en bedrift som har hatt mye problemer med datavirus de siste månedene. En stor del av grunnen til virusproblemene er at brukerne har for liten kunnskap om hva et datavirus er, og hvordan det fungerer. Du skal derfor skrive en enkel informasjon som forklarer

- hva et datavirus er
- hvordan brukeren skal unngå at maskinen får virus
- hvordan brukeren kan oppdage at maskinen har fått et datavirus
- hva brukeren skal gjøre når han har mistanke om at maskinen har fått et datavirus

Du må ta hensyn til at mange av brukerne har liten kunnskap om IKT generelt, og at brukerne stort sett ikke vet mer om datavirus enn det de har lest i aviser eller hørt på radio eller sett på TV.

Drift og vedlikehold

Plan for systeminstallasjoner

Planlegge en systeminstallasjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Planlegge en systeminstallasjon (124689)

Planleggingen av en systeminstallasjon starter med at vi vurderer hvilke nåværende og framtidige behov løsningen skal dekke.

Systeminstallasjoner organiseres ofte som prosjekter. Før du begynner, bør du derfor vite litt om prosjektorganisering. Dette er omtalt i faget *Virksomhetsstøtte* i kompetansemålet "Hente informasjon, gi råd og veilede i forbindelse med planlegging av nye systemløsninger i en virksomhet".

Planleggingen av en systeminstallasjon starter med at vi vurderer hvilke nåværende og framtidige behov løsningen skal dekke. Installasjonen må selvsagt dekke det behovet virksomheten har i dag, men vi må også ta hensyn til hvilke behov virksomheten antakeligvis får i framtida.

Avhengig av størrelsen på installasjonen kan dette være et omfattende arbeid. Lista under viser noen av de vanligste spørsmålene som må avklares i forbindelse med planleggingen.

Hvor mange brukere kommer installasjonen til å ha?

For å kunne beregne hvor mange maskiner installasjonen skal ha, hvor mange servere, hvor mange nettverksuttak, hvor mange programlisenser og så videre, må du først vite hvor mange brukere den kommer til å få. Videre må du ta hensyn til eventuell framtidig vekst slik at det ikke oppstår kapasitetsproblemer hvis virksomheten får flere ansatte eller kunder.

I utgangspunktet kan det virke som en forholdsvis enkel oppgave å beregne antall brukere, men du må ta hensyn til hva slags installasjon det er snakk om, og hva den skal brukes til.

Hvis det for eksempel er et lokalnettverk, vil det ofte bare være ansatte som er brukere, men hvis løsningen inkluderer en internettjeneste, må du også beregne hvor mange samtidige brukere som det er sannsynlig at vil benytte tjenesten.

Hvor mange servere eller tjenere skal nettverket ha?

Begrepet server, eller tjener på norsk, kan i IKT-sammenheng bety både en fysisk maskin og en tjeneste i et nettverk.

For å skille dem fra hverandre bruker vi ofte betegnelser som filserver, databaseserver, skriverserver, webserver, e-postserver, proxyserver, og så videre når vi snakker om servertjenester, og nettverkserver eller bare server om en fysisk maskin.

For å kunne beregne størrelsen på installasjonen må du vite antall brukere. Fotograf: Lise Åserud

Facebooks nye serverhall i Luleå, Sverige. Fotograf: Susanne Lindholm

Bruken av betegnelsene er imidlertid ikke konsekvent, og ofte blir den fysiske maskinen omtalt med navnet på den tjenesten den hovedsakelig leverer. Det er også vanlig at flere servertjenester kjøres fra den samme fysiske maskinen, slik at denne kan bli omtalt med ulike betegnelser avhengig av hvilken tjeneste man viser til.

Når vi planlegger en systeminstallasjon som skal inkludere én eller flere servere, er det viktig å skille mellom servertjenester og fysiske maskiner for å unngå misforståelser.

- Hvilke servertjenester skal være tilgjengelige i nettverket?
- Hva slags maskin eller maskinkapasitet krever servertjenestene?

I et lite nettverk er det ikke uvanlig at mange eller alle servertjenestene kjører på den samme fysiske maskinen, mens i et stort nettverk kan det være behov for å spre én enkelt tjeneste på mange fysiske maskiner for å klare å betjene alle brukerne. Store selskaper som Google og Facebook har flere hundre tusen servere samlet i store datasenter over hele verden for å klare å betjene sine brukere.

Hvor mange datamaskiner skal kobles til nettverket lokalt?

Det er ikke nødvendigvis slik at antallet brukere er det samme som antall maskiner. Det kan for eksempel være brukere som har behov for flere maskiner, eller flere brukere som skal dele den samme maskinen. Det siste er vanlig i virksomheter med skiftarbeid og på arbeidsplasser hvor datamaskiner brukes til å slå opp eller registrere data i forbindelse med annet arbeid, for eksempel i butikker eller på lager.

Det kan også være behov for maskiner som ikke skal ha noen definerte brukere. Eksempler på slike kan være maskiner som står som informasjonskiosker, som skal styre produksjonsmaskiner eller brukes til spesielle oppgaver.

Hvor mange andre enheter skal kobles til nettverket eller inngå i installasjonen?

Andre enheter inkluderer utstyr som skrivere, skannere, tilgangspunkter for WiFi, avbruddsfrie strømforsyninger, utstyr for sikkerhetskopiering med mer.

Hvordan skal nettverket kobles til Internett?

De fleste nettverk skal ha en tilkobling til Internett, og du må vurdere hva slags internettilknytning det er behov for, hvor stor kapasitet som kreves, og hvilke sikkerhetsutfordringer tilkoblingen skaper. Det siste er grundig behandlet i kompetansemålene ”Vurdere systeminstallasjoner mot krav til tilgjengelighet, informasjonssikkerhet og helse, miljø og sikkerhet” og «”Aktivisere, vurdere og dokumentere sikkerhetsmekanismer for å forebygge og varsle forsøk på sikkerhetsbrudd”.

Har brukere behov for ekstern tilgang til nettverket? Hvordan skal de i så fall få det?

Selv om en systeminstallasjon ikke skal tilby tjenester via Internett, kan det være brukere som har behov for ekstern tilgang, for eksempel hvis virksomheten har flere avdelinger eller brukere som har hjemmekontor eller er mye på reise.

Skal nettverket ha mulighet for trådløs tilgang?

Hvis brukerne har bærbare maskiner, kan det være behov for trådløs nettverkstilgang i tillegg til vanlig kablet tilgang. Trådløs tilgang kan også være nødvendig for gjester.

Hva slags operativsystem skal server i nettverket bruke?

Valg av operativsystem for servere er et svært viktig punkt fordi det også er operativsystemet for selve nettverket. Serveroperativsystemer kalles derfor ofte for nettverksoperativsystem, forkortet NOS.

Opplegg for hjemmekontor kan kreve ekstra planlegging av IKT-medarbeideren.
Fotograf: Kerstin Mertens

Type programvare er med på å avgjøre systemets kapasitet.
Fotograf: Jan-Philipp Strobel

Valg av NOS begrenser blant annet hvilke programmer som kan kjøres i nettverket, og er avgjørende for hvilken kompetanse administratorer må ha.

Microsoft er et av firmaene som lisensierer ut sine programmer.
Fotograf: Niall Carson

Hvilke serverbaserte programmer skal kjøres i nettverket? Hva er maskinvarekravene til disse?

Planen må inkludere en oversikt over hvilken programvare som skal installeres på servere og kjøres i nettverket.

Dette er også viktig av hensyn til planlegging av kapasiteten. Store databasesystemer, videoredigeringsverktøy, programmer for simuleringer, teknisk tegning og lignende krever betydelig mer prosesseringskapasitet, lagringsplass og nettverkskapasitet enn vanlige kontorstøttesystemer.

Hva slags operativsystem og programmer skal brukermaskiner i nettverket ha?

Den vanligste løsningen for installasjon av operativsystem og programvare på brukermaskiner er å lage en «masterinstallasjon», kalt en «image», som legges på server. Imagen er en fullstendig installasjon av operativsystem og programvare som kan overføres til brukermaskinene via nettverket.

Lenke: Desktop Deployment

Hva er maskinvarekravene til de lokale programmene?

På samme måte som for serverne må du finne ut hvilke maskinvarekrav de programmene som skal kjøres lokalt på brukermaskinene, har. Det kan være nødvendig å lage flere spesifikasjoner siden ikke alle brukere alltid har de samme behovene.

Hvor mange programlisenser må virksomheten kjøpe til servere og brukermaskiner?

Når du har oversikt over hvilke programmer som skal brukes i nettverket, og hvor mange brukere installasjonen vil få, kan du beregne hvor mange lisenser du trenger for hvert program.

Vi ønsker ikke å betale for flere lisenser enn vi trenger, men vi må også være sikre på at vi ikke bruker programmer uten å betale for dem.

Programvarelisenser kan være knyttet til

- antall brukere totalt
- antall samtidige brukere
- antall maskiner programmet er installert på

For en lisens som er knyttet til **antall brukere,** skal vi betale en lisens for hver person som bruker programmet, men hver bruker kan godt ha programmet installert på flere maskiner.

For en lisens som er knyttet til **antallet samtidige brukere,** skal vi bare betale for så mange som bruker programmet samtidig. Slike lisenser benyttes for mange serverbaserte programmer. Hvis vi for eksempel har lisens for 20 samtidige brukere av et program og alle lisensene er i bruk, vil en ny bruker ikke få tilgang til programmet før en annen logger seg ut.

For en lisens som er knyttet til **antall maskiner programmet er installert på,** skal vi betale for antallet installasjoner uavhengig av hvor mange som bruker programmet.

Det finnes også programmer som har en kombinasjon av flere lisenstyper.

Planlegge den fysiske nettverksinstallasjonen

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Planlegge den fysiske nettverksinstallasjonen (124707)

Skal en helt ny nettverksinstallasjon planlegges, må også den fysiske installasjonen settes opp.

Hvis det er snakk om en helt ny nettverksinstallasjon, må også den fysiske nettverksinstallasjonen designes og planlegges. Viktige spørsmål å få avklart i forbindelse med dette er:

- Hvilken nettverkstopologi skal nettverket ha? (Hvordan skal for eksempel noder i datanettverket kobles sammen med kabler, og hvor skal de plasseres i bygget?)
- Hva slags kabel skal nettverket bruke?
- Hvor mange tilkoblingspunkter for maskiner og utstyr skal nettverket ha?
- Hvordan skal nettverkskablene trekkes?
- Hvor skal tilkoblingspunktene plasseres?
- Hva slags nettverksutstyr er det behov for?
- Hvor skal nettverksutstyr plasseres?
- Hvor skal servere plasseres?
- Hvor skal nettverksskrivere og annet tilkoblet utstyr plasseres?

Merk at nettverksdesign krever kunnskap som går utover pensum for videregående skole, og det bør derfor gjøres i samarbeid med en nettverksdesigner. Videre bør den fysiske kablingen som regel overlates til et kabelinstallasjonsfirma.

Kabeltyper

En vanlig brukt kabeltype for lokalnettverk er tvunnet parkabel kategori 5, men over lengre avstander kan fiberkabel eller koaksialkabel være aktuelt. Fiberkabel brukes også ofte mellom nettverksutstyr og til servere for å øke hastigheten i nettverket og responstiden fra servere.

Nettverksutstyr

Nettverksutstyr er alt utstyr som brukes til det fysiske kabelnettet. Det kan inkludere huber, rutere, broer og svitsjer. Behovet for og valget av nettverksutstyr er avhengig av en rekke faktorer, blant annet:

- hva slags nettverkstopologi nettverket har
- hvor mange segmenter (deler) nettverket skal deles opp i
- hva slags kabel nettverket bruker
- avstanden mellom ytterpunktene i nettverket
- hvor mange noder (maskiner og annet utstyr) som skal tilkobles
- den fysiske plasseringen av maskiner og utstyr
- hvilken hastighet dataoverføringen i nettverket skal ha
- hvilke sikkerhetskrav det er til nettverket

Ved trekking av nettverkskabel og plassering av nettverksutstyr må vi også ta hensyn til eventuelle **bygningstekniske krav** eller begrensninger. Det kan for eksempel være brannvegger som det ikke er lov å trekke kabel gjennom, eller behov for ventilasjon i skap eller rom hvor nettverksutstyr skal stå.

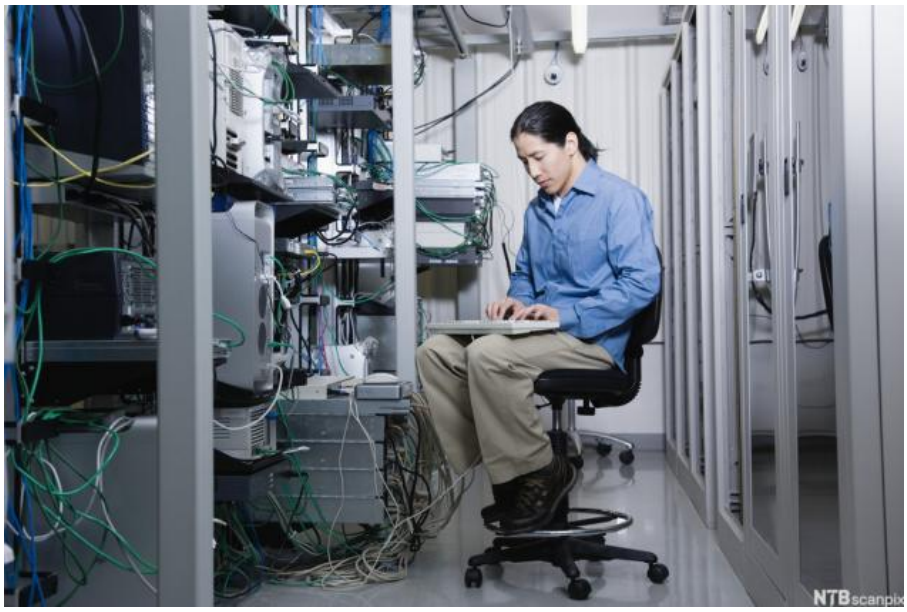
Planlegge sikkerhet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Planlegge sikkerhet (124709)

Ved alle systeminstallasjoner er det viktig å tenke sikkerhet helt fra starten av, slik at sikkerhet er bygget inn i installasjonen og ikke blir noe som legges til som en ettertanke etter at installasjonen er ferdig.

Viktig sikkerhetsspørsmål som må få svar når vi planlegger installasjonen, er blant annet:

- Hvilke sikkerhetstiltak mot angrep skal servere og nettverk ha (antivirus, passord, brannmur, demilitarisert sone, datakryptering og så videre)?
- Hvordan skal servere, brukermaskiner og nettverksutstyr sikres fysisk?
- Hvordan skal sikkerhetskopiering gjøres, og hvilken kapasitet må utstyr for sikkerhetskopiering ha?
- Er det utstyr som trenger avbruddsfri strømforsyning?



Sikkerheten må planlegges nøye før bygging av serverrom.

Fotograf: Corbis

Disse og andre sikkerhetsvurderinger er behandlet i kompetansemålene "Vurdere systeminstallasjoner mot krav til tilgjengelighet, informasjonssikkerhet og helse, miljø og sikkerhet" og "Aktivisere, vurdere og dokumentere sikkerhetsmekanismer for å forebygge og varsle forsøk på sikkerhetsbrudd"

Nettverksdiagram

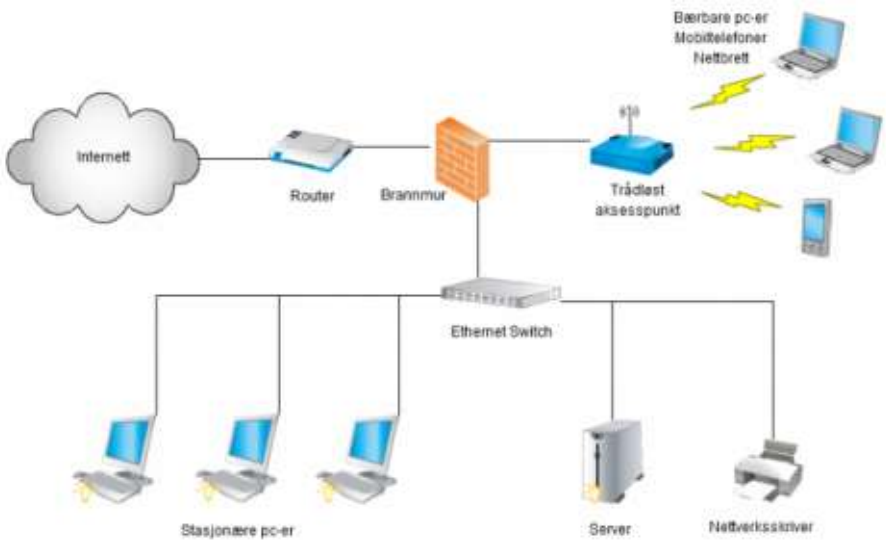
Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Nettverksdiagram (124711)

Planleggingen av en systeminstallasjon bør inkludere nettverksdiagrammer og plantegninger for kabelstrekk og plassering av maskiner og utstyr.

Et nettverksdiagram er en oversiktstegning over nettverket, mens plantegninger viser hvor maskiner, utstyr, kabler og tilkoblingspunkter er fysisk plassert i lokalene.

Nettverksdiagram kan lages i programmer som Visio. Det finnes også nettbaserte verktøy som for eksempel Creately.com.

Eksempel på et enkelt nettverksdiagram ser du under.



Eksempel på enkelt nettverksdiagram.

Opphavsmann: Arne Jansen

Beregne kostnadene for installasjonen

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Beregne kostnadene for installasjonen (124715)

Når installasjonen er planlagt, må vi beregne og budsjettere kostnadene.

Vi kan dele kostnadene for en systeminstallasjon inn i

- anskaffelseskostnader
- installasjonskostnader
- implementeringskostnader
- servicekostnader
- opplæringskostnader

For større installasjoner må det ofte også til håndverkere som elektrikere og snekkere for å få alt på plass.
Fotograf: Claudio Bresciani

Opplæring av ansatte er viktig for å lykkes med nye installasjoner.
Fotograf: Berit Keilen

Anskaffelseskostnader

Anskaffelseskostnadene er den prisen vi må betale for maskiner, utstyr og programvare som skal inngå i installasjonen.

Installasjonskostnader

Installasjonskostnader er kostnader for selve installasjonen av utstyr og programvare. Dette omfatter både interne kostnader i form av timer for ansatte og kostnader til eksterne leverandører eller konsulenter som nettverksdesigner, kabelinstallatør, systemleverandør, elektriker, snekker og så videre. I tillegg til installasjonskostnadene kommer også eventuelle kostnader til testing av installasjonen.

Implementeringskostnader

Hvis installasjonen skal inngå som en del av et eksisterende system, kan det være kostnader forbundet med å tilpasse systemene til hverandre. Tilpassing til eksisterende løsninger kan for eksempel være kommunikasjon med annet utstyr, datautveksling mellom ulike programmer og lignende. Slike kostnader kan være vanskelige å identifisere på forhånd.

Servicekostnader

Servicekostnader er forventede kostnader til teknisk service og serviceavtaler. Dette er ofte eksterne kostnader som timepris for en servicetekniker eller en årlig serviceavtale med et fast beløp.

Opplæringskostnader

Nye systemer krever alltid opplæring. I tillegg til brukerne må IKT-medarbeidere som skal ha ansvar for drift og brukerstøtte, også få grundig opplæring i forkant av installasjonen.

Budsjettering og beregning av kostnader ved en systeminstallasjon er nærmere beskrevet i kompetansemålet ”Dokumentere investerings- og driftskostnader for systeminstallasjoner”.

Planlegge utrulling og fallback

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Planlegge utrulling og fallback (124718)

For nye systeminstallasjoner i et eksisterende nettverk må selve utrullingen også planlegges slik at driften ikke forstyrres mer enn absolutt nødvendig. I tillegg må det finnes en fallback-løsning i tilfelle noe går galt.

Å gjennomføre en større systeminstallasjon eller oppgradering kalles gjerne for en utrulling og krever at det lages en utrullingsplan.

En utrulling av nye systeminstallasjoner må planlegges slik at de forstyrrer pågående arbeid minst mulig.

Fotograf: Science Photo Library

Utrullingsplanen skal vise

- hva som skal rulles ut til hvilke brukere
- en tidsplan for utrullingen
- en oversikt over hvilke aktiviteter som må gjennomføres i forbindelse med utrullingen
- hvem som har ansvaret for å utføre de ulike oppgavene under utrullingen

Selv om en løsning er testet på forhånd, kan det alltid skje noe som gjør at installasjonen feiler. I så fall må det finnes en plan for hvordan man skal komme tilbake til situasjonen slik den var før installasjonen startet. Dette kalles ofte en fallback-løsning.

Lenke: Eksempel på

Utrullingsplan / fil
http://ndla.no/nb/node/124716

Program- og maskinvare

Innhente tilbud og anskaffe utstyr

Forfatter: Arne Jansen, NKI Forlaget
Innhente tilbud og anskaffe utstyr (127232)

Planene for systeminstallasjonen som vi lagde i det forrige kompetansemålet, er utgangspunkt for kravdefinisjoner og kravspesifikasjoner når vi skal hente inn tilbud fra utstyrsleverandører.

Utstyret må dekke behovet

Det viktigste når vi kjøper inn utstyr til en systeminstallasjon, er ikke prisen, men at utstyret dekker de behovene virksomheten har. Vi må derfor være nøye med å spesifisere hvilke krav vi har til utstyret, hva det skal brukes til, og hvilket utstyr det skal kobles sammen med.

Når vi skal kjøpe inn datautstyr, er det viktig å følge reglene for anskaffelser. Du kan lese om regler for anskaffelser her.

Når vi skal investere i nytt datautstyr, må vi vite hva vi trenger – hvilke behov virksomheten vår har.

Kravdefinisjon og kravspesifikasjon

Krav til IKT-systemer kan beskrives enten som en kravdefinisjon eller som en kravspesifikasjon.

En kravdefinisjon er en brukerorientert beskrivelse av et IKT-system, mens en kravspesifikasjon er en presis teknisk beskrivelse av det samme systemet.

En kravdefinisjon skrives i vanlig språk slik at den er forståelig for alle som er involvert. Kravene deles inn i to kategorier: **funksjonelle** og **ikke-funksjonelle krav.**

Funksjonelle krav er en beskrivelse av hvordan systemet skal «oppføre» seg, hva det skal gjøre og ikke gjøre, og sier noe om tilgjengelighet, brukervennlighet og sikkerhet fra brukerens ståsted.

Ikke-funksjonelle krav er rammene for systemet. For en nettverksinstallasjon kan det for eksempel være hastighet, antall brukere, antall tilknytningspunkter og lignende. De ikke-funksjonelle kravene skiller seg fra de funksjonelle ved at det er mulig å tallfeste dem.

Kravdefinisjon og kravspesifikasjon er omtalt i faget *Virksomhetsstøtte* i kompetansemålet *«Kartlegge behov for IKT-støtte i en arbeidsprosess og utarbeide en kravdefinisjon for et IKT-system».*

Merk at det også er vanlig at leverandører deltar i planleggingsarbeidet.

Det viktigste ved anskaffelse av utstyr til en systeminstallasjon er ikke prisen, men at utstyret dekker de behovene virksomheten har.

Installere programvare og maskinvare

Forfatter: Arne Jansen, NKI Forlaget
Installere programvare og maskinvare (127247)

Denne delen av kompetansemålet er av praktisk art og må ta utgangspunkt i hvilket maskinutstyr og hvilken programvare du har tilgang til.

Når vi skal installere program- og maskinvare, er det mye å tenke på. Vi må ta hensyn til drivere, maskinkrav til programvare, behov, plan for installasjonen, brukerdokumentasjon og så videre. Er vi bevisste på alle disse aspektene og følger installasjonsplanen nøye, sparer vi mye tid seinere.

Å installere program- og maskinvare kan være litt av et puslespill – det er mange biter som skal passe sammen!

Installasjonsplan

Ved installasjon er det viktig å ha en godt gjennomarbeidet plan. Installasjonsplanen bør vise:

- hvilket utstyr og hvilken programvare som skal installeres
- i hvilken rekkefølge utstyret og programvaren skal installeres og konfigureres
- hvordan utstyr og programvare skal konfigureres
- hvordan sikkerhet skal konfigureres, inklusive tilganger og rettigheter
- hvordan installasjonen skal testes underveis og til slutt

Du må også undersøke hvilke drivere du trenger til nettverkskort, skrivere og eventuelt annet utstyr. Windows har drivere for svært mange nettverkskort og skrivermerker, men det kan være nødvendig å laste ned oppdaterte drivere fra leverandørenes nettsider.

Med en god og gjennomtenkt installasjonsplan sparer vi mye tid seinere.

Liten nettverksinstallasjon

Forfatter: Arne Jansen, NKI Forlaget
Liten nettverksinstallasjon (127263)

Her skal vi ta for oss en installasjon av et lite nettverk. Installasjonen må ta utgangspunkt i hvilket maskinutstyr og hvilken programvare du har tilgang til.

Vi beskriver ikke selve installasjonen og konfigureringen her, siden den er avhengig av type utstyr og operativsystemversjoner som skal brukes. Du må derfor ta utgangspunkt i informasjon og handbøker for det utstyret og den programvaren du skal bruke.

Følg nøye instruksjonen i handboka for maskiner og programvare.

Hva trenger du?

For å kunne gjennomføre en liten nettverksinstallasjon trenger du:

- en maskin som kan fungere som server
- minimum to maskiner som kan fungere som brukermaskiner
- en hub eller switch
- kabler og plugger
- en skriver
- et nettverksoperativsystem (Windows-server eller Linux)
- et standard kontorstøttesystem (Officepakke)
- tilgang til Internett (for å kunne laste ned drivere, søke i leverandørers online-dokumentasjon og lignende)

Hva må du gjøre?

Oppgaver du bør gjennomføre i forbindelse med installasjonen omfatter å

- planlegge rekkefølge for installasjon og konfigurasjon
- installere nettverksoperativsystem på server
- installere kontorstøttesystem på server
- lage en mappestruktur på server
- opprette og konfigurere rettigheter og tilganger for brukerkontoer
- installere operativsystem på brukermaskiner
- koble server og brukermaskiner sammen med hub eller switch
- installere skriverservertjeneste på en av brukermaskinene
- koble skriver til hub eller switch
- konfigurere sikkerhet på server og arbeidsstasjoner

Teste installasjonen

Når installasjonen er fullført, bør du teste at:

- brukermaskinene kan kommunisere med server
- brukere kan logge inn
- tilganger og rettigheter er satt riktig for ulike brukere
- kontorstøttesystem på server kan kjøres fra brukermaskinene
- utskrift fungerer fra brukermaskinene
- sikkerhetsinnstillinger fungerer

Ansatte sjekker at maskinene kommuniserer med serveren etter installasjonen.

Du må selvsagt også teste den enkelte installasjonen underveis før du går videre til neste punkt i installasjonsplanen.

Utvide installasjonen

Avhengig av hvilket utstyr du har tilgang til, kan du utvide installasjonen. Her er noen muligheter:

- I en klasse kan flere små nettverk kobles sammen til ett nettverk med flere segmenter.
- Ulike servertjenester som for eksempel e-post og web kan installeres på en eller flere servere.
- Hvis nettverket kan kobles til Internett, kan tjenester for VPN og ekstern tilgang til for eksempel en nettserver konfigureres.
- Du kan konfigurere en maskin som brannmur og sette opp en demilitarisert sone DMZ med en server foran og en bak brannmuren.
- Hvis du har tilgang til flere rutere, kan det settes opp flere mulig rutere mellom to eller flere LAN-nettverk.
- Du kan sette opp et WiFi-tilgangspunkt for trådløs tilgang til nettverket.

Å planlegge er en viktig del av installasjonen og ved utvidelse av installasjonen.

Funksjoner i et IKT-system

Dokumentere en systeminstallasjon

Forfatter: Arne Jansen, NKI Forlaget
Dokumentere en systeminstallasjon (127269)

En systeminstallasjon må dokumenteres, og dokumentasjonen må oppdateres når det skjer endringer.

Gjennom å dokumentere installasjonen grundig kan vi spare oss for både tid og ergrelser seinere. Å dokumentere er kanskje ikke den mest spennende av oppgavene til en IKT-medarbeider, men god dokumentasjon er helt nødvendig for at vi skal kunne gjøre en god jobb.

Dokumentasjonsbehov

Vi kan dele inn dokumentasjonsbehovet i fem hovedgrupper:

- systemdokumentasjon av nettverk og utstyr (IKT-systemer)
- dokumentasjon av driftsoppgaver og rutiner
- dokumentasjon av arbeidsprosesser og informasjonsflyt
- dokumentasjon av brukerstøtte
- informasjon og dokumentasjon for brukere

I det følgende skal vi se nærmere på det første punktet: dokumentasjon av nettverk og utstyr.

Hvor er feilen? God systemdokumentasjon hjelper oss til å rette opp feil raskere.

IKT-medarbeider i serverrommet. Installasjoner og endringer dokumenteres fortløpende.

Dokumentasjon av driftsoppgaver og rutiner er omtalt i kompetansemålet «*Planlegge, utføre og dokumentere driftsoppgaver og daglig vedlikehold av en systeminstallasjon*».

Dokumentasjon av arbeidsprosesser og informasjonsflyt er omtalt i faget «Virksomhetsstøtte» i kompetansemålene «*Dokumentere IKT-bruk og vurdere kostnads- og nytteverdien av et IKT-system*» og «*Kartlegge behov for IKT-støtte i en arbeidsprosess og utarbeide en kravdefinisjon for et IKT-system*».

Dokumentasjon av brukerstøtte er omtalt i faget «Bruker- og driftsstøtte» i kompetansemålet *«Dokumentere hvordan en intern eller ekstern brukerstøttefunksjon er organisert og fungerer»* og i faget «Virksomhetsstøtte» i kompetansemålet *«Gjennomføre og dokumentere en analyse av henvendelser til brukerstøtte for å avdekke behov for endringer, opplæring og brukerveiledninger».*

Informasjon og dokumentasjon til brukere er omtalt i faget «Bruker- og driftsstøtte» i kompetansemålet «*Dokumentere og gjøre tilgjengelig løsninger på problemer».*

Hvorfor dokumentere?

Forfatter: Arne Jansen, NKI Forlaget
Hvorfor dokumentere? (127293)

Det kan i utgangspunktet virke overflødig å dokumentere så mye, men god systemdokumentasjon gir mange fordeler.

Mange tenker at det er unødvendig med så mye dokumentasjon, bare systemet virker, er alt ok. Men oppstår det feil, er det mye raskere å finne feilen når du har god dokumentasjon. Dessuten blir det lettere for andre å overta hvis du for eksempel bytter jobb!

Med god dokumentasjon blir det enklere å finne feilen!

Hjelp ved feilsøking

Når noe går galt, vil systemdokumentasjonen være en verdifull referanse i feilsøkingsprosessen. God dokumentasjon reduserer tida som går med til feilsøking. Det er gjerne slik at de nettverkene som har mest problemer, også er de med minst dokumentasjon - og omvendt.

Hjelp for nye IKT-medarbeidere

De fleste bytter på ett eller annet tidspunkt jobb. Når en ny medarbeider overtar ansvaret for systemet, vil dokumentasjonen være vesentlig for at den nye medarbeideren skal få oversikt over systemet.

Hjelp for leverandører og konsulenter

Ved seinere utvidelser vil leverandører eller konsulenter ofte ha behov for en oversikt over systemet.

Bedre oversikt

Datautstyret er en del av bedriftens inventar. Derfor skal det verdisettes i regnskapet og som regel avskrives. Bedriften eier ofte også maskiner og annet utstyr som disponeres av de ansatte utenfor arbeidsplassen. Det er derfor et behov for å holde oversikt over hvor dette utstyret befinner seg, og hvem som disponerer det.

Programvarelisenser er gjerne knyttet opp mot antallet brukere, eller antallet maskiner programmet er installert på. Support- og serviceavtaler er ofte knyttet opp til bestemte maskiner eller et bestemt antall maskiner.

Mange jobber utenfor selve arbeidsplassen og disponerer maskiner som bedriften eier. Dette må vi ha oversikt over.

Selv om det er litt arbeid å lage og vedlikeholde en god systemdokumentasjon, sparer det på sikt IKT-medarbeiderne for mye tid og virksomheten for penger.

Planlegg dokumentasjonen

Forfatter: Arne Jansen, NKI Forlaget
Planlegg dokumentasjonen (127388)

God planlegging er alltid viktig. Hva bør dokumenteres, og hvordan skal det presenteres? Hvor detaljert er det nødvendig at systemdokumentasjonen er?

Dokumentasjon = kommunikasjon

Å dokumentere et system kan kreve litt planlegging. Dokumentasjon er først og fremst en kommunikasjonsoppgave. Du skal dokumentere teknisk informasjon om et system på en slik måte at du seinere enkelt kan finne tilbake til den informasjonen du trenger, og slik at andre skal kunne lese og forstå den. Det er ikke sikkert at det som er opplagt for deg, er opplagt for en annen ansatt som skal bruke dokumentasjonen seinere.

Dokumentasjon er kommunikasjon. Sørg derfor for at dokumentasjonen er forståelig for andre!

Detaljnivå

Samtidig må ikke systemdokumentasjonen bli så detaljert og omfattende at det blir håpløst å finne den informasjonen man trenger. Husk også at dokumentasjonen må oppdateres hver gang det skjer endringer. Hvis detaljnivået blir for høyt, blir oppdateringsjobben også tilsvarende stor.

Du må derfor tenke igjennom hva som bør dokumenteres, og hvordan informasjonen bør presenteres, slik at dokumentasjonen blir enkel å bruke og å vedlikeholde.

Tenk over

Hva hadde du trengt å vite hvis du skulle overta ansvaret for et system som du ikke kjente fra før? Det er dette du bør dokumentere.

Litt er bedre enn ingenting!

Det kan virke overveldende å ta fatt på en systemdokumentasjon. Noen kommer aldri i gang fordi de er usikre på hvor de skal begynne, eller de er redde for at de ikke skal klare å gjøre det riktig. Men husk at selv en mangelfull dokumentasjon er bedre enn ingen dokumentasjon. Å dokumentere et IKT-system er også nyttig for å lære systemet bedre å kjenne.

Gjør litt av dokumentasjonen hver dag - så blir jobben mer overkommelig.

Hvor lang tid det tar å dokumentere, er avhengig av størrelsen på og kompleksiteten til systemet. Det kan være lurt å sette av litt tid hver dag eller hver uke istedenfor å forsøke å gjøre hele jobben i en omgang.

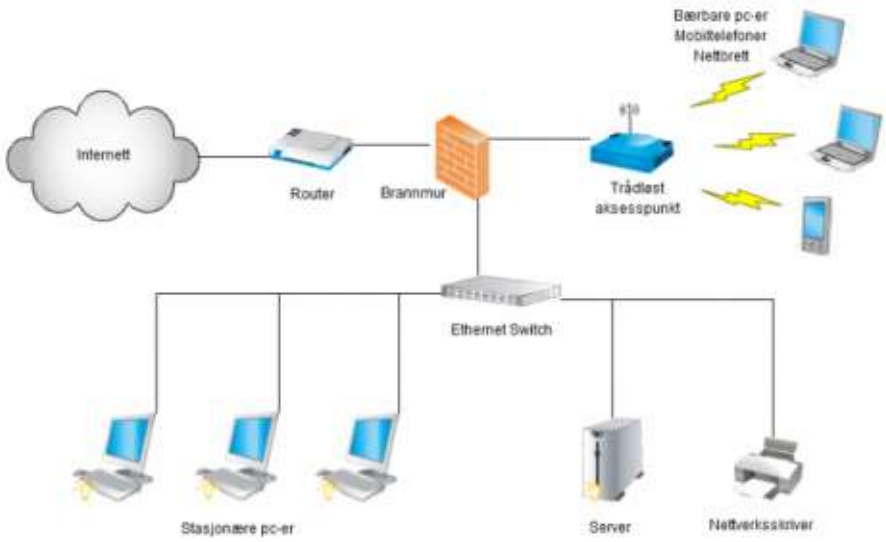
Dokumentasjon er kommunikasjon og krever planlegging. Husk også at andre skal kunne bruke dokumentasjonen seinere.

Hva skal du dokumentere?

Forfatter: Arne Jansen, NKI Forlaget
Hva skal du dokumentere? (127401)

IKT-systemer er forskjellige, men de har likevel mye felles. Det gjør at vi kan lage en liste over hva vi må tenke på når vi skal dokumentere systemet.

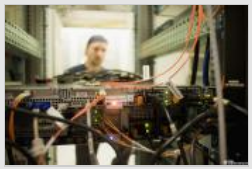
Alle IKT-systemer er unike, men de har likevel mange fellestrekk. Oversikten nedenfor viser hva du bør vurdere å dokumentere.



Eksempel på et enkelt nettverksdiagram.

- **Nettverkstopologi**

  Dette dokumenterer vi vanligvis i form av et diagram som viser de mest sentrale nodene i nettverket og hvordan de er koblet sammen - typisk servere, rutere, svitsjer og brannmurer. I tillegg bør du inkludere hvor kabler er trukket, hvor sentrale koblingspunkter befinner seg, og plasseringen av uttak for maskiner. Det kan også være nødvendig å dokumentere hva slags kabler som er bruk i ulike deler av nettet (type og kapasitet).
  Det er gjerne hensiktsmessig å benytte en plantegning over den bygningen som nettverket omfatter, og merke av kabelstrekk og koblingspunkter på denne. I et nettverk som er kablet i henhold til de anbefalinger og spesifikasjoner som gjelder for lokalnettverk, skal alle kabler og koblingspunkter også være merket, slik at hvert uttak har en unik id (for eksempel et nummer). Disse id-ene bør også være med i dokumentasjonen.



Det kan være nødvendig med dokumentasjon av kabeltyper og kapasitet.

- **Serverinformasjon**
  Dette omfatter servernavn og funksjon (filserver, e-postserver, webserver og så videre), IP-adresse(r), disk-konfigurasjon, operativsystem, leverandør, garanti, serviceavtale og så videre.
-
- **Serverkonfigurasjoner**
  omfatter rettigheter og tilganger i nettverket (Active Directory for Windows servere).
-
- **Ruter- og brannmurkonfigurasjon**
  Dette omfatter IP-adresser, ruterkonfigurasjon, brannmurregler, internettilkobling, internettleverandør og ekstern tilgang for ansatte (VLAN).

-
- **Konfigurasjon av nettverkstjenester**
  - blant annet DNS (Domain Name System) og DHCP (Dynamic Host Configuration Protocol).
-
- **Kritiske programmer**
  Dette gjelder hvilke programmer som brukes i nettverket og eventuelle spesielle krav til utstyr. Hvem som bruker programmene, og hvem som er leverandøren.
-
- **Programvarelisenser**
  Du må ha oversikt over hva slags lisenser virksomheten har for alle programmer, og hvilke begrensninger lisensene har.
-
- **Sikkerhetspolicy inklusive rutiner for sikkerhetskopiering**
  Dette er omtalt i kompetansemålene *"Vurdere systeminstallasjoner mot krav til tilgjengelighet, informasjonssikkerhet og helse miljø og sikkerhet"* og *"Aktivisere, vurdere og dokumentere sikkerhetsmekanismer for å forebygge og varsle forsøk på sikkerhetsbrudd".*

Husk at systemdokumentasjonen også må sikres mot innsyn fra uvedkommende.

Automatisert dokumentasjon

Forfatter: Arne Jansen, NKI Forlaget
Automatisert dokumentasjon (127408)

Det finnes flere verktøy som sørger for automatisk systemdokumentasjon. Det letter nok arbeidet noe, men du må som regel ha et manuelt register også.

Verktøy for automatisk dokumentasjon

Det finnes flere verktøy som automatisk registrerer maskiner og utstyr som er koblet i et nettverk. Det er også mulig å hente inn opplysninger automatisk om konfigurasjon av den enkelte maskin og hvilke programmer som er installert.

Videre har Windows innebygget verktøy for å dokumentere Active Directory, og det finnes også flere tredjepartsverktøy tilgjengelig.

Verktøy for automatisk generering av systemdokumentasjon forenkler dokumentasjonsarbeidet betydelig, men i tillegg må du normalt vedlikeholde et manuelt register også.

Det vil alltid være utstyr som systemene ikke vil være i stand til å registrere, for eksempel passivt nettverksutstyr (utstyr som ikke har noen egen adresse i nettverket) eller tilkoblet utstyr som skjermer, skrivere og skannere. I tillegg kommer maskiner og utstyr som ikke er koblet til nettverket. Typisk er brukeres hjemmemaskiner.

Det mest hensiktsmessige er som regel en enkel database eller et regneark som inneholder informasjon om

- merke, modell og serienummer på maskiner og nettverksutstyr
- plassering av utstyret
- leverandøren
- innkjøpsdato og garantitid
- utstyret omfattes av service eller supportavtaler
- hvem som eventuelt disponerer utstyret

Hold dokumentasjonen så oversiktlig som mulig. Bruk illustrasjoner og tabeller der det er mulig.

Brukeres hjemmemaskiner som ikke er tilkoblet nettverket, må dokumenteres i et manuelt register.

Hold informasjonen oppdatert!

Systemdokumentasjon må oppdateres hver gang det skjer endringer som gjør at den ikke lenger er korrekt. Foreldet informasjon kan i noen tilfeller være verre enn ingen informasjon i det hele tatt.

- Oppdater systemdokumentasjonen med én gang. Jo lenger du utsetter det, jo større er risikoen for at det ikke blir gjort.
-
- Informasjon som er "ferskvare", bør ha en "best før"-dato. Det vil si at den er tydelig merket med en dato for når den ikke lenger er aktuell.
-
- All informasjon bør dateres tydelig slik at det er mulig å se hvor gammel den er, og når den sist ble oppdatert.
-

Det er enklere å være IKT-servicemedarbeider dersom dokumentasjonen er oversiktlig og oppdatert!

- All dokumentasjon bør ha en person som er ansvarlig for at den oppdateres.

Lenke til Network Topology Mapper

> Verktøy for automatisk kartlegging av nettverket forenkler dokumentasjonsarbeidet betydelig.

Kostnadskontroll

Budsjettere investerings- og driftskostnader

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Budsjettere investerings- og driftskostnader (109198)

Det er ikke IKT-servicemedarbeideren som skal utarbeide virksomhetens budsjett, og det forventes normalt ikke at du har økonomibakgrunn i stillingen som IKT-servicemedarbeider. Men det er heller ikke uvanlig at du må delta i budsjettarbeidet for IKT-avdelingen.

I det minste må du kunne si noe fornuftig om hvilke kostnader og investeringer du regner med at driften av IKT-systemene vil påføre virksomheten i framtiden. Grunnleggende kjennskap til noen av de vanlige ordene og begrepene som benyttes i forbindelse med budsjettering, kan derfor komme godt med.

Hva er et budsjett?

Et budsjett kalles ofte et **forhåndsregnskap**. Når vi fører regnskap, registrerer vi hva vi har brukt penger til, og hvor inntektene har kommet fra i løpet av en periode. Et budsjett sier noe om hva vi har tenkt å bruke penger til i framtiden, og hvilke inntekter vi forventer at kommer. En annen måte å betrakte et budsjett på er å si at det er **virksomhetens planer uttrykt i kroner**.

Det er to faktorer som det er viktig for en bedrift å få oversikt over i budsjettet: resultatet og likviditeten. **Resultatet** sier om virksomheten kommer til å gå med overskudd eller underskudd, mens **likviditeten** er uttrykket for hvor mye penger man til enhver tid har. Vi setter derfor gjerne opp et **resultatbudsjett** og et **likviditetsbudsjett**. Grunnlaget for disse to budsjettene er virksomhetens forventede inntekter, kostnader og investeringer.

Resultatbudsjettet og likviditetsbudsjettet bruker altså de samme tallene som utgangspunkt, men det er én viktig forskjell. Resultatbudsjettet forteller virksomheten hvilke kostnader og inntekter den vil ha, mens likviditetsbudsjettet forteller *når* kostnadene må betales, og når inntektene kommer inn. Dette er vesentlig fordi virksomheten kan ha behov for finansiering for å klare å betale sine regninger til riktig tid, selv om den på sikt kommer til å ha et positivt resultat.

Fotograf: Berit Roald

Når du skal arbeide med å kartlegge IKT-kostnader, kan det være lurt å bruke et **regneark**. Her kan du repetere det du lærte om regneark på Vg1.

Husker du dette om **budsjett?**

Budsjett og avviksanalyse

Hva er et budsjett?

En virksomhet som skal budsjettere, må derfor vite hvilke kostnader IKT-avdelingen vil pådra seg i det kommende året, hvilke investeringer den må gjøre, og når de må gjøres.

Utgangspunktet for et budsjett er gjerne de kostnadene man hadde i foregående budsjettperiode, slik at det er eventuelle endringer i forhold til det normale som det vil være viktigst å få med. I forbindelse med virksomhetens budsjettbehandling må vi derfor kunne svare på følgende:

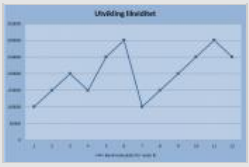
- Hvilke IKT-kostnader ut over de som løper fast, må vi regne med i kommende periode?
- Hvilke IKT-investeringer er planlagt?
- Når forfaller de ulike IKT-kostnadene og investeringene til betaling?

Dersom du for eksempel vet at bedriften til neste år skal investere i nye laptoper til alle ansatte, eller kjøpe inn et helt nytt regnskapssystem, må kostnadene til disse investeringene synliggjøres i budsjettet for neste år.

Hvis du arbeider for en virksomhet som selger IKT-tjenester, vil selvsagt inntektene du regner med å generere, også være av stor betydning.

Du bør kunne si noe fornuftig om hvilke kostnader og investeringer du regner med at driften av IKT-systemene vil påføre virksomheten i framtiden.

Det kan være nyttig at du venner deg til å lese og tolke regneark når du skal arbeide med IKT-kostnader.
Fotograf: Corbis



Slik kan utviklingen i din bedrifts likviditet vises grafisk. Her kan du lese ut av grafen hvor mye penger bedriften har tilgjengelig hver måned i året. Penger som for eksempel skal brukes til å betale leverandører og lønninger til de ansatte.
Opphavsmann: Oddvar Torgersen

Et innkjøp av nye laptoper til hele bedriften vil utgjøre en stor investeringskostnad som må med i budsjettet.
Fotograf: Simon Chavez

Kostnad eller investering?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kostnad eller investering? (109201)

I regnskapet skiller vi mellom kostnader og investeringer. Det er regler for hva som regnes som kostnader, og hva som skal ses på som investeringer.

En **investering** kan defineres som en driftsanskaffelse som koster mer enn 15 000 kroner (eksklusive merverdiavgift) og som har en forventet brukstid på tre år eller mer. En **kostnad** blir dermed en anskaffelse som koster mindre enn 15 000 kroner eller har en forventet brukstid på mindre enn tre år.

Legg merke til at både kostnader og investeringer som regel må betales med én gang eller i løpet av kort tid. Forskjellen ligger i at investeringer fortsetter å ha en verdi over tid, mens de varene eller tjenestene virksomheten forbruker med en gang, er kostnader.

Avskriving

Hvis en virksomhet for eksempel kjøper en ny nettverksserver til 35 000 kroner, må den selvsagt betale hele beløpet ved anskaffelsen. Men siden serveren representerer en verdi, kan ikke virksomheten kostnadsføre hele beløpet med en gang. I stedet må serveren **avskrives** i regnskapet over flere år slik at kostnadene fordeles etter hvert som serveren blir mindre verdt.

Avskriving betyr rett og slett at vi hvert år reduserer verdien på en gjenstand i regnskapet fordi den blir eldre og mer slitt. I praksis betyr det at kostnaden blir fordelt over flere år.

Et viktig poeng er at en virksomhet får **fradrag** for de kostnadene den har til driften. Disse fradragene gjør at det skattepliktige resultatet blir lavere og virksomheten må betale mindre skatt. Både myndigheter og virksomheter er derfor opptatt av at avskrivinger blir gjort korrekt.

Driftsmidler

Utstyr som skal avskrives, kalles for **driftsmidler**. Driftsmidler er eiendeler som forbrukes over tid (mer enn tre år). Dette gjelder ikke bare datamaskiner, men også annet utstyr som produksjonsmaskiner, biler, driftsbygninger osv.

For virksomhetens skatteregnskap er det egne regler for hvordan ulike typer driftsmidler skal avskrives. En bil faller for eksempel ikke like fort i verdi som en datamaskin. Kontormaskiner, som er den kategorien datautstyr hører til, har derfor en ganske høy avskrivingssats på 30 %. Verdien av en ny datamaskin skal altså reduseres i regnskapet med 30 % av innkjøpsprisen hvert år.

Utstyr som koster mindre enn 15 000 kroner, kan kostnadsføres i sin helhet ved anskaffelse, selv om ustyret har en lengre levetid enn ett år. En bærbar datamaskin til 6000 kroner kan vare like lenge som en server, men fordi den koster mindre enn 15 000 kroner, vil den bli utgiftsført som en kostnad i regnskapet med en gang.

Innkjøp av nye servere må budsjetteres.
Fotograf: David Selman

En firmabil er et eksempel på et driftsmiddel, det er også ulike typer kontormaskiner.
Fotograf: Thorfinn Bekkelund

Lenke:

Sjekk reglene for avskriving – artikkel fra miniforetak.no

Det oppstår av og til usikkerhet når en virksomhet kjøper flere datamaskiner samtidig, for eksempel fem bærbare maskiner til 6000 kroner per stykk. Siden grensen for investeringer som skal avskrives, går ved 15 000 kroner, og hver maskin bare koster 6000 kroner, kan det være naturlig å anta at alle maskinene skal kostnadsføres med en gang. Men den totale investeringen for alle de fem maskinene er på 30 000 kroner. Og når man kjøper flere enheter av samme type utstyr slik at summen blir over 15 000 kroner, skal det regnes som en investering som skal avskrives selv om den enkelte enhet ikke koster over 15 000 kroner. Forutsetningen er selvsagt fortsatt at utstyret har en brukstid på minst tre år.

En investering er en driftsanskaffelse som koster mer enn 15 000 kroner og som har en forventet brukstid på tre år eller mer.

IKT-innkjøp

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
IKT-innkjøp (109209)

Større innkjøp og investeringer må planlegges på forhånd. Det er en rekke faktorer som bør være avklart før du bestiller hvis du vil unngå overraskende og ofte unødige kostnader.

Det er naturlig at IKT-medarbeidere i en virksomhet er involvert i de IKT-innkjøpene og investeringene virksomheten må gjøre. Det å bestille en datamaskin krever selvsagt ikke noen omfattende kunnskaper, men ved litt større investeringer må vi være mer påpasselige.

For det første er virksomheten interessert i å få mest mulig igjen for de investeringene den skal gjøre, samtidig som kostnadene holdes nede. Her vil du som IKT-servicemedarbeider kunne bidra fordi du er i en posisjon hvor du kan forutse eventuelle problemer og identifisere kostnader som ledelsen ikke har forutsetninger for å kunne se. For eksempel når det gjelder utstyr som begynner å bli gammelt og som snart må skiftes ut.

Større innkjøp og investeringer må planlegges på forhånd, og det er en rekke faktorer som bør være avklart før du bestiller hvis du vil unngå overraskende og unødige kostnader. Punktene under er ment som en sjekkliste. Alle punktene vil ikke nødvendigvis være aktuelle for alle typer anskaffelser, men de gir en oversikt over hva du bør være oppmerksom på:

Konsekvenser

- Hvilke konsekvenser vil en investering i nytt utstyr medføre for eksisterende systemer? Vil for eksempel investeringen føre til at annet utstyr eller programvare må oppgraderes?
- Vil det være behov for å legge om eksisterende rutiner eller etablere nye rutiner?

Levering, installasjon og igangkjøring

- Når skal levering foregå?
- Hvem besørger og betaler for levering?
- Stiller utstyret spesielle krav til lokaler? For eksempel krav til fysisk sikkerhet mot skade eller uautorisert tilgang? Er det behov for temperatur-/fuktighetsregulering? Hvor mange nettverkstilknytninger eller strømuttak kreves?
- Hvem har ansvaret for å pakke opp utstyret og montere det? Kreves det for eksempel tekniker fra leverandør?
- Når skal montering og igangkjøring gjennomføres? Må dette for eksempel gjøres utenom vanlig arbeidstid for å unngå at annet arbeid forstyrres?
- Hvem bekoster montering og igangkjøring?
- Hvilke personer må være til stede eller tilgjengelige i forbindelse med igangkjøring og testing?
- Hvis utstyret skal fungere sammen med eksisterende IKT-systemer i virksomheten, hvem har da ansvaret for at dette fungerer?
- Vil det være behov for å overføre data fra eksisterende systemer, og hvem er eventuelt ansvarlig for at dette gjøres?
- Hvilke kriterier skal gjelde for overdragelse av ansvaret? Det vil si: Når skal utstyret anses for å være levert?

Dokumentasjon

- Hvilken dokumentasjon følger med utstyret?
- Vil det være behov for å utarbeide egen dokumentasjon for brukere?
- Vil det være behov for å dokumentere nye rutiner eller endre dokumentasjonen for eksisterende rutiner?

Behovet for opplæring

- Hvilket behov for opplæring vil investeringen medføre for brukere og for IKT-personell?
- Er det behov for eget kursmateriell?
- Når skal opplæringen foregå?

- Kan opplæring gjøres internt eller kreves det eksterne kurs?
- Hvem skal bekoste opplæring?

Vedlikehold og service

- Hvor lang servicetid må vi regne med fra leverandøren ved en eventuell feil?
- Finnes det reservedeler eller reserveutstyr tilgjengelig?
- Bør virksomheten selv ha reservedelslager?
- Er det behov for en egen serviceavtale på utstyret?

Garantier

- Hvilke garantibetingelser følger utstyret?
- Hva kan vi selv foreta oss med hensyn til service og tilpassinger innenfor garantien?

Betalingsbetingelser

- Hvilke betalingsbetingelser får vi? Ved investeringer som også inkluderer utvikling av programsystemer, er det for eksempel ikke uvanlig at man betaler deler av regningen underveis.

Som du ser, vil mange av punktene over involvere leverandøren, og mange av dem kan ha en høy kostnad i forhold til prisen på utstyret eller programmet. For eksempel vil ofte installasjon, igangkjøring, tilpassing og opplæring være langt mer kostnadskrevende ved anskaffelse av et nytt programsystem enn prisen på selve applikasjonen. Det er derfor vesentlig å avklare med leverandøren hvem som skal dekke de ulike kostnadene, og hvem som har ansvaret når noe eventuelt ikke fungerer som det skal.

Det er viktig å avklare med leverandøren hvem som skal dekke de ulike kostnadene, og hvem som har ansvaret når noe eventuelt ikke fungerer som det skal.

Drift og vedlikehold

Driftsoppgaver og daglig vedlikehold

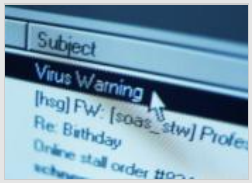
Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Driftsoppgaver og daglig vedlikehold (124523)

En av IKT-medarbeiderens arbeidsoppgaver er å vedlikeholde virksomhetens ikt-system. Ved å sørge for regelmessig vedlikehold av maskiner, servere, nettverksutstyr, program og tilganger oppstår det færre akutte problemer, og oppdateringer og utskifting av utstyr kan planlegges på forhånd.

Vanlige drifts- og vedlikeholdsoppgaver inkluderer

- å kjøre sikkerhetskopiering og kontrollere at kopien kan kopieres tilbake
- å sjekke sikkerhetslogger og hendelseslogger på servere
- å overvåke ressurser som kan være en begrensning eller bli en flaskehals
- å installere sikkerhetsoppdateringer og andre programoppdateringer
- å vedlikeholde brukerkontoer og tilganger
- å resette passord for brukere
- å bytte passord på servere
- å kontrollere at alle sikkerhetstiltak fungerer som de skal

Dette er bare en oversikt over de vanligste oppgavene, og listen er på ingen måte utfyllende. Drifts- og vedlikeholdsoppgaver for IKT-system vil variere avhengig av maskinutstyr, programvare, nettverk og bruk.



Det er viktig med kontinuerlig vedlikehold, blant annet for å unngå større virusangrep. Fotograf: Science Photo Library

Driftslogg

Du bør dokumentere hvilke drifts- og vedlikeholdsoppgaver som blir utført, når de ble gjort, og hvem som utførte dem. Dette gjøres vanligvis i en driftslogg. Å føre driftslogg er spesielt viktig når virksomheten har mer enn én IKT-medarbeider, slik at andre kan se hva som er blitt gjort.

En driftslogg er vanligvis bare et dokument, et regneark eller en database der alle aktiviteter blir skrevet inn i kronologisk rekkefølge. Hvis det er mange driftsoppgaver, kan det lønne seg å dele inn loggen slik at oppgaver som hører sammen, står samlet – ett ark for det som gjelder sikkerhetskopiering, et annet for bytte av passord for brukere, og så videre.

Eksempel på en enkel driftslogg

Driftslogg - brukeradministrasjon				
Dato	Kl.	Oppgave	Status	Utført av
12.06.2013	13:00	Resatt passord for Geir Graabein.	OK	Christian
12.06.2013	12:00	Gitt Line Lissom lesetilgang til markedsavdelingens fellesområde. Godkjent av markedssjef.	OK	Christian
11.06.2013	15:00	Fjernet brukerkonto for vikar på ordrekontoret.	OK	Thomas
09.06.2013	10:00	Opprettet standard brukerkonto for Line Lissom, nyansatt i salgsavdelingen. Forespørsel fra salgsdirektør.	OK	Thomas

Sikkerhetskopiering

Back-up for Google på lager i Berkeley, USA. Fotograf: Connie Zhou

En sentral del av de daglige driftsoppgavene er sikkerhetskopiering. Sikkerhetskopier må tas regelmessig, og det må finnes en rutine som sikrer at kopieringen blir utført riktig, at kopiene oppbevares trygt, og at det er mulig å legge kopien tilbake hvis data går tapt.

Sikkerhetskopiering er grundig behandlet i kompetansemålet Vurdere systeminstallasjoner mot krav til tilgjengelighet, informasjonssikkerhet og helse, miljø og sikkerhet, og rutiner for sikkerhetskopiering er forklart i faget "Bruker og driftsstøtte" i kompetansemålet Yte service gjennom driftsstøtte og kommunikasjon med leverandører og fagpersonell på norsk og engelsk. Her skal vi derfor bare oppsummere kort hva som bør ligge til grunn for en god rutine for sikkerhetskopiering:

- hvor ofte sikkerhetskopiering skal kjøres
- når sikkerhetskopiering skal kjøres
- hva slags sikkerhetskopiering som skal utføres
- hva det skal tas kopi av
- hvem som er ansvarlig for at sikkerhetskopiering kjøres
- hvem som overtar hvis den ansvarlige ikke er tilgjengelig
- hvordan sikkerhetskopieringen utføres
- hvordan kontroll av at sikkerhetskopieringen er i orden, skal gjøres
- hvor og hvordan sikkerhetskopier skal oppbevares
- hvordan en eventuell tilbakekopiering utføres
- hvem som er ansvarlig for å oppdatere rutinen og kontrollere at den blir fulgt

Ressursovervåking

Hong Kong børs er et eksempel på en bedrift der ressurstilgangen kontinuerlig overvåkes, slik at de ansatte alltid har kapasitet nok til å få gjennomført transaksjoner og kommunisert med sine klienter. Fotograf: Imaginechina

En annen vanlig driftsoppgave er ressursovervåking. Vi overvåker ressurser i nettverket som kan være en begrensning eller bli en flaskehals.

Ressurser som overvåkes, er vanligvis:

- Lagringsplass: harddiskplass på servere og arbeidsstasjoner, samt kapasitet på media for sikkerhetskopiering
- Nettverkskapasitet: tilstrekkelig hastighet på internt nettverk og internettilgang
- Serverkapasitet: serverparkens mulighet til å betjene det forventede antallet brukere og forespørsler
- Skriverressurser: tilstrekkelig kapasitet til å håndtere bedriftens utskriftsvolum

Serveroperativsystem har innebygget funksjoner for å måle ressursbelastning. Det finnes også mange spesialiserte program og verktøy for ressursovervåking. Selve informasjonsinnsamlingen er vanligvis automatisert, slik at belastningen på ulike ressurser registreres automatisk på fastsatte tidspunkter.

Ressursovervåking er også viktig for å kunne forutse og planlegge framtidige behov for oppgraderinger og utvidelser.

Dette temaet er også behandlet i faget ”Bruker og driftsstøtte” i kompetansemålet Yte service gjennom driftsstøtte og kommunikasjon med leverandører og fagpersonell på norsk og engelsk.

Ved å sørge for regelmessig vedlikehold oppstår det færre akutte problemer, og oppdateringer og utskifting av utstyr kan planlegges på forhånd.

Servervedlikehold

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Servervedlikehold (124535)

Servervedlikehold innebærer å sørge for at en server fungerer optimalt. Manglende vedlikehold fører over tid til dårligere ytelse, dårligere sikkerhet og hyppigere feil.

Servervedlikehold kan deles inn i tre hovedoppgaver:

- systemovervåking
- installasjon av oppdateringer
- regelmessig planlagt vedlikehold

Facebooks nybygde serverhall i Luleå i Sverige. Dette skal bli navet i Facebooks verdensomspennende nett. Fotograf: Susanne Lindholm

Systemovervåking

Nettverksoperativsystem (NOS) og mange servere, som e-postservere, webservere, databaseservere og så videre, har funksjoner for logging av hendelser og aktiviteter som kan være av betydning for IKT-ansvarlig. Det finnes også en rekke spesialprogram for server- og nettverksovervåking.

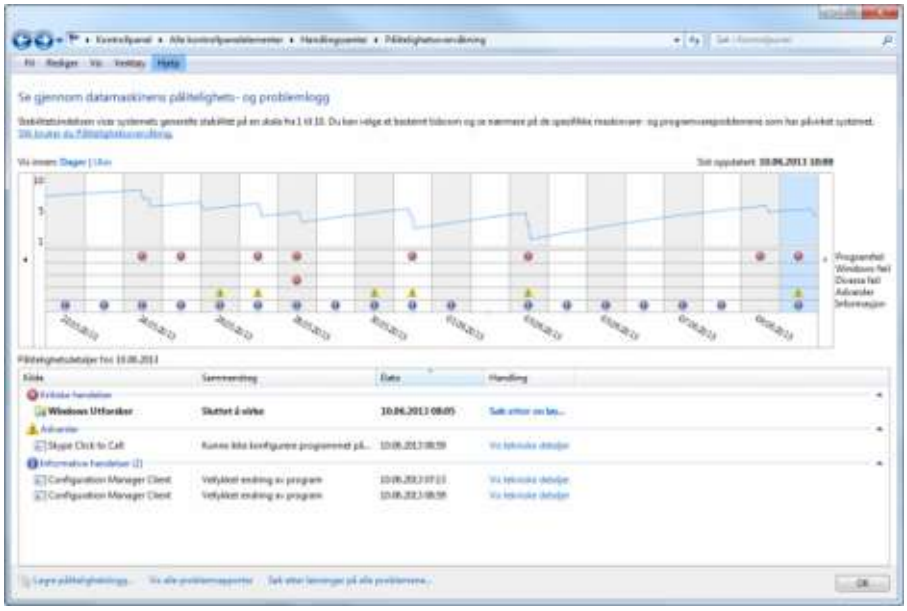
Lenke: Eksempel på spesialprogramvare for overvåking av servere og nettverk

Vi er vanligvis interessert i å logge informasjon om tre typer hendelser:

1. **Autentisering:** når noen logger seg på eller av, eller forsøker å gjøre det
2. **Trafikk:** hvilke forespørsler serveren mottar, hvor forespørslene kommer fra, og hva de gjelder
3. **Systemproblemer**

Windows' server har følgende innebygde standardlogger:

- **Application Log** registrerer hendelser for program, som for eksempel en database som ikke kan aksesseres.
- **System Log** registrerer hendelser som gjelder selve operativsystemet.
- **Security Log** registrerer hendelser som pålogging, filaksess og annet relatert til datasikkerhet.
- **Directory Service Log** registrerer hendelser logget av Active Directory og tilhørende tjenester.
- **DNS Server Log** registrerer all DNS-aktivitet.
- **File Replication Service Log** registrerer replikeringsaktivitet i systemet.



Skjermdump av datamaskinenes pålitelighets- og problemlogg.

Opphavsmann: Microsoft

Legg merke til at systemovervåking ikke er det samme som kapasitetsovervåking. Verktøy for systemovervåking logger hendelser, mens verktøy for kapasitetsovervåking logger belastning og ytelse.

Selv om det kan være overlappende områder, brukes systemloggene først og fremst for å oppdage programfeil og sikkerhetsbrudd.

Det er også viktig å være klar over at selv om du har tilgang til å logge all aktivitet i nettverket, betyr ikke det at du alltid skal gjøre det. Systemovervåking kan komme i konflikt med personvernloven og brukernes rettigheter selv om hensikten er å avdekke feil eller sikkerhetsbrudd. Denne problemstillingen er forklart i faget "*Bruker og driftsstøtte*" i kompetansemålet Behandle fortrolige opplysninger på en etisk forsvarlig måte innenfor rammene av gjeldende regelverk .

Det er for eksempel vanlig å registrere hvem som har forsøkte å logge seg på en server, og om det ble godtatt eller ikke. Det er også vanlig å logge hvem som til enhver tid bruker ulike filer og program, internettaktivitet og utskrifter.

Slike logger kan brukes til systemadministrasjon og sikkerhet, men hvis virksomheten vil bruke informasjonen til noe annet, må den først få samtykke fra de ansatte.

Siden det er IKT-medarbeidere som vanligvis er ansvarlige for systemlogger og skal utføre selve overvåkingen, er det viktig at du kjenner disse reglene godt og vet hva du kan og ikke kan gjøre.

Oppdateringer og planlagt vedlikehold

Når det skal utføres vedlikehold eller oppdateringer på servere, må de ofte kobles fra nettverket. Slikt vedlikehold blir derfor vanligvis gjort i helger eller utenfor vanlig arbeidstid, slik at det skaper minst mulig avbrudd for brukerne.

Hvor hyppig vedlikehold må gjøres, er avhengig av hvilke oppgaver serveren har, og hvor stor belastning den utsettes for, men normalt gjøres det to–fire ganger per år. Hvis det er behov for hyppigere vedlikehold, er det ofte et tegn på at serveren blir overbelastet.

Fra et serverrom i Yandex data i Russland.

Fotograf: Alexander Ryumin , ITar-Tass

En plan for servervedlikehold må inkludere installasjon av programoppdateringer. I motsetning til vanlige pc-er, der oppdateringer ofte installeres fortløpende, bør oppdatering av programvaren på en server planlegges på forhånd og følge fastlagte rutiner.

Vi må kunne være sikre på at alle oppdateringer som gjøres på servere, fungerer som de skal, og at vi eventuelt kan komme tilbake til situasjonen slik den var før oppdateringene ble gjort, hvis noe ikke fungerer. En typisk rutine for oppdatering av en server kan være

- å ta en fullstendig sikkerhetskopi av hele serveren
- å koble serveren fra nettet og installere oppdateringen
- å teste om alle program fungerer som de skal etter oppdateringen
- hvis det er flere oppdateringer, installere en og en og teste serveren mellom hver oppdatering
- koble serveren til nettet igjen.

Hvis en oppdatering ikke fungerer slik den skal, eller hvis den har uventede konsekvenser, må den fjernes og sikkerhetskopien legges tilbake.

Vi må kunne være sikre på at alle oppdateringer som gjøres på servere, fungerer som de skal, og at vi eventuelt kan komme tilbake til situasjonen slik den var før oppdateringene ble gjort, hvis noe ikke fungerer.

Vedlikeholdsplan

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vedlikeholdsplan (124539)

Vedlikeholdsplanen skal sørge for at nødvendig vedlikehold skjer regelmessig, og at noen er ansvarlig for vedlikeholdet, slik at det ikke blir tilfeldige oppgaver som bare blir gjort når det oppstår en feil.

Drifts- og vedlikeholdsoppgaver skal utføres regelmessig og bør organiseres som faste rutiner, slik at du kan være sikker på at de blir utført som planlagt, og kan kontrollere at de blir gjort riktig.

En vedlikeholdsplan skal inneholde en oversikt over hvilket utstyr som må vedlikeholdes, hva som skal gjøres regelmessig, og hvor hyppig vedlikeholdet skal utføres.

Merk at program og operativsystem også må vedlikeholdes og oppdateres. De fleste programvareprodusenter kommer med serviceoppdateringer etter hvert som de oppdager feil, eller i forbindelse med endringer i operativsystem eller applikasjoner. Oppdatering av operativsystem og programvare er grundig behandlet i kompetansemålet Aktivisere, vurdere og dokumentere sikkerhetsmekanismer for å forebygge og varsle forsøk på sikkerhetsbrudd.

Eksempel på vedlikeholdsplan

Vedlikeholdsplanen bør settes opp på årsbasis og skal vise

- hva som skal gjøres
- hvor ofte det skal gjøres
- når det skal gjøres
- hvor lang tid det normalt vil ta
- hvordan brukerne blir påvirket

Oppgave	Når	Start	Lengde	Innvirkning på drift
Sikkerhetskopiering	Alle dager	01:00	3 timer	Redusert responstid for brukerne
Kontroll og arkivering av sikkerhetskopi	Alle hverdager	09:00	30 min.	Ingen
Sikkerhetslogg	Alle hverdager	09:30	15 min.	Ingen
Systemlogg	Ukentlig	Fredager kl. 09:45	15 min.	Ingen
Restart av server	Månedlig	Siste fredag i måneden kl. 18:00	30 min.	Ingen servertjenester eller data tilgjengelig for brukerne
Sikkerhetstest	Månedlig	Siste fredag i måneden	1 time	Redusert responstid for brukerne
Antivirus oppdatering	Daglig	07:00	10 min.	Ingen
Programoppdateringer	Kvartalsvis	Første lørdag i kvartalet	3 timer	

				Ingen servertjenester
Passordbytte på server	Månedlig	Første mandag i måneden	15 min.	eller data tilgjengelig for brukerne
Maskinvareoppgraderinger	Ved behov	Ved behov	Ukjent	Ingen servertjenester eller data tilgjengelig for brukerne
...				
...				

Eksempel på vedlikeholdsplan. Opphavsrett: Arne Jansen

Merk at dette er en forkortet utgave av en vedlikeholdsplan. En komplett plan vil inkludere langt flere oppgaver og kan også inneholde mer informasjon, for eksempel hvem som er ansvarlig for oppgaven, og hvordan oppgaver som påvirker brukerne, skal varsles.

Vedlikeholdsplanen skal sørge for at vedlikehold skjer regelmessig, og at noen er ansvarlig for vedlikeholdet.

Driftsavtaler og serviceavtaler

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Driftsavtaler og serviceavtaler (124541)

På grunn av kostnadene til driftsstøtte, og for å redusere lønnskostnadene, velger mange virksomheter å sette bort driftsstøtten til et eksternt firma som har spesialisert seg på dette.

Det finnes flere firma som tilbyr driftsstøtte enten på timebasis, som periodisk vedlikehold eller som faste driftsavtaler der det eksterne firmaet har ansvaret for alt vedlikehold og it-drift. Mange firma tilbyr også fjernadministrering (fjerndrift) av virksomhetens nettverk.

Som for luftambulansen er responstiden kritisk også for firmaer som tilbyr ulike typer IKT-service.
Fotograf: Lise Åserud

De fleste maskinprodusenter og mange programvareleverandører tilbyr i tillegg dedikerte serviceavtaler for sine produkter.

Det finnes også firma som tilbyr såkalte katastrofeløsninger, der virksomhetens servere replikkeres til et eksternt driftssenter hver natt. Hvis det skjer noe som gjør at serverne blir ødelagt, for eksempel ved en brann, kan serverne startes opp igjen fra driftssenteret.

Et vesentlig punkt i serviceavtaler er garantert **responstid**. Typisk vil en avtale garantere at en tekniker er på plass og har startet jobben med å løse problemet innen et spesifisert antall timer etter at problemet er varslet.

Et vesentlig punkt i serviceavtaler er garantert responstid.

Krav

Tilgjengelighet eller sikkerhet?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Tilgjengelighet eller sikkerhet? (113828)

Det er nødvendig å finne en balanse mellom kravene til datasikkerhet og behovet for brukervennlige systemer.

Det blir sagt at det å trekke ut nettverkskabelen og slå av maskinen er den eneste løsningen for å beskytte en datamaskin helt mot datavirus, hacking, datatyveri, uautorisert tilgang eller andre sikkerhetsbrudd.

Siden det vanligvis ikke er en praktisk løsning å gjøre det, må vi akseptere at kravene til sikkerhet alltid må vurderes opp mot brukernes behov for enkel tilgang og brukervennlige systemer.

På den ene siden ønsker vi å ha så god sikkerhet som mulig. På den annen side ønsker vi at systemene skal være så tilgjengelige og brukervennlige som mulig. For dårlig sikkerhet gjør systemene sårbare for datatap og driftsavbrudd, men hvis sikkerheten er for streng, kan systemene bli så tungvinte at de er mer til ulempe enn til nytte.

Et økende behov for kommunikasjon og datautveksling gjør at mange virksomheter må åpne opp stadig flere av systemene sine for nye brukere og bruksområder, og de må gjøre informasjon tilgjengelig på nye måter og steder. Dette skaper store utfordringer for IKT-ansvarlige som skal ivareta sikkerheten i systemene.

IKT-ansvarlige legger vanligvis mest vekt på sikkerheten, siden det å beskytte virksomhetens systemer og sensitive data er et ansvar man må ta alvorlig. I mange tilfeller er sikkerhet også lovpålagt, og slurv kan i verste fall føre til straffereaksjoner fra myndighetene – for eksempel ved for dårlig sikring av dataregistre som inneholder personinformasjon.

Virusangrep.
Fotograf: Science Photo Library

Sikkerhetsutfordringene – som for eksempel virus og hacking – har endret seg mye de siste årene.
Fotograf: Egil Eikvil

Hvilke ulemper kan det for eksempel være ved å bruke **samme passord** på mange ulike tjenester, slik det offentlige nå ønsker å gjøre?

Husker du dette om personvern?

Brukerne på sin side er gjerne mest opptatt av at IKT-systemene er lett tilgjengelige og enkle å bruke. Du kan heller ikke forvente at brukere er kjent med den teknologien og de teknikkene som brukes for datasikkerhet.

Som IKT-medarbeider må du derfor finne en balanse mellom kravene til sikkerhet og behovet for brukervennlige systemer.

Økende behov for kommunikasjon og datautveksling skaper store utfordringer for IKT-ansvarlige som skal ivareta sikkerheten.

Databruk i endring og sikkerhetsbevisste brukere

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Databruk i endring og sikkerhetsbevisste brukere (113834)

Utviklingen innen mobilteknologi og nettbasert databehandling skaper store utfordringer for en som er ansvarlig for IKT-sikkerhet.

Tidligere handlet sikkerhetstiltak først og fremst om å skape en barriere mellom virksomhetens datasystemer og omverdenen. Vanlige tiltak var brannmurer, systemer for tilgangskontroll, fysisk beskyttelse og overvåking av nettverkstrafikk.

Men utviklingen innen mobilteknologi med smarttelefoner, nettbrett, trådløse nettverk og programmer og data i nettskyen (cloud computing), har gjort det nesten umulig å isolere virksomhetens data fra omverden.

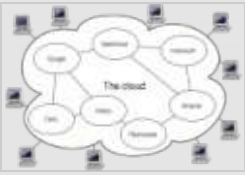
Det fører ikke bare til at det blir vanskeligere for virksomhetens egne IKT-medarbeidere å opprettholde sikkerheten. De må i stadig større grad også stole på at andre ivaretar sikkerheten.

Hvis en virksomhet for eksempel bruker nettsky-tjenester (cloud computing), som Google Disk, DropBox, SlideShare eller en av de tusenvis av andre tilsvarende tjenestene på nettet, er virksomheten avhengig av at leverandøren av tjenesten sørger for sikkerheten.

Videre har smarttelefoner, nettbrett og andre mobile datamaskiner gjort brukerne mindre avhengige av virksomhetens datautstyr. Stadig flere bruker like gjerne sine egne telefoner og maskiner i jobbsammenheng og installerer egne programmer og app-er.

Dette kan skape store problemer for IKT-avdelingen, som ikke har mulighet for å ivareta sikkerheten for utstyr som virksomheten ikke eier. Mange velger å forby bruk av alle enheter og programmer som ikke er godkjent av virksomheten, men det har også sine ulemper og kan skape nye problemer og misfornøyde brukere.

Brannmur som beskyttelse mot virus.
Fotograf: Science Photo Library



Cloud computing.
Opphavsmann: Sam Johnston

Brukerne må vite hvordan de skal – og ikke skal – oppbevare passordene sine.
Fotograf: Victor Bayon

Hvis sikkerhetsrutinene oppfattes som så strenge og tungvinte at brukerne føler at de ikke lenger får gjort jobben sin på den enkleste måten, vil de etter hvert finne måter å omgå sikkerheten på. Hvis du for eksempel innfører så strenge krav til passord at det blir vanskelig for brukerne å huske passordene sine, vil mange begynne å skrive ned passordene og oppbevare dem i nærheten av maskinen. Dermed risikerer du at et tiltak som skulle gi bedre sikkerhet, i praksis fører til at sikkerheten blir dårligere.

For å komme ut av denne klemmen og unngå at datasikkerhet blir et stridstema, må

- IKT-medarbeidere anstrenge seg for å forstå brukernes behov for tilgjengelige systemer
- ledelsen og brukerne bli bevisste på at de også selv har et ansvar for å ivareta sikkerheten

Det kan for eksempel bety at du må akseptere dårligere sikkerhet for systemer og data som ikke er så kritiske. Brukeren på sin side må akseptere strengere sikkerhetsrutiner for de mest sårbare systemene og de mest sensitive dataene.

Hvis sikkerhetsrutinene oppfattes som så strenge og tungvinte at brukerne føler at de ikke lenger får gjort jobben sin på enkleste måte, vil de etter hvert finne måter å omgå sikkerheten på.

Narvik.

Fotograf: Helge Sunde

Narvik-saken

Våren 2011 besluttet Narvik kommune seg for å gå over til Googles nettsky-tjenester (Google Apps) for e-post, kalender og dokumentutveksling for over 1500 ansatte.

Narvik var den første kommunen i Norge som valgte å satse på en slik nettsky-tjeneste, og det ble ikke godt mottatt hos Datatilsynet. Datatilsynet mente at personvernet ikke ville bli godt nok ivaretatt fordi kommunen mistet kontrollen over personopplysninger når de overlot det ansvaret til Google.

Datatilsynet var også skeptiske til at Google, som et amerikansk selskap, ikke er underlagt norske regler for personvern, og at kommunen dermed ikke kunne vite hvor opplysningene ble lagret, eller hvem som fikk tilgang til dem. Datatilsynet gav derfor Narvik kommune beskjed om at kommunen måtte si opp avtalen med Google.

Narvik kommune klaget på vedtaket og forsikret Datatilsynet om at Google Apps ikke ville bli brukt til saksbehandling eller sensitive saksopplysninger. Videre informerte Narvik kommune innbyggerne sine om at de ikke får sende sensitive opplysninger til kommunen via e-post. Høsten 2012 snudde Datatilsynet.

Datatilsynet understreker imidlertid at selv om Narvik nå har fått godkjent bruk av nettsky-tjenester, er det ikke fritt fram for alle kommuner eller offentlige etater.

Lenker

- Narvik velger Google apps – Digi.no, 9. mai 2011
- Sier nei til Google apps – Computerworld, 24. januar 2012
- Datatilsynet snur i Narvik-saken – Computerworld, 24. september 2012

Sikre soner

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikre soner (113835)

I stedet for å prøve å beskytte alle data like godt velger mange virksomheter etter hvert å være mer fleksible.

I praksis blir det gjort ved at man skiller de viktigste systemene fra de mindre viktige og oppretter en **sikker sone** for sensitiv informasjon og kritiske data. Man kan for eksempel velge å benytte fysisk adskilte tjenere eller separate nettverk. På den måten kan man ha de nødvendige sikkerhetstiltakene for den sikre sonen, samtidig som mindre viktige systemer kan være lett tilgjengelige.

Det er lettere å få aksept fra brukerne for strenge sikkerhetstiltak for sensitive data når det er tydelig at det er nødvendig med sikkerhet, og når brukerne ikke får problemer med tilgjengeligheten til mindre sensitive systemer.

I en sikker sone kan man legge flere sikkerhetslag, alt avhengig av behovet for sikkerhet. Eksempler på sikkerhetstiltak kan inkludere:

- fysisk atskilte tjenere
- separat nettverk
- frakoblet Internett
- ingen tilgang via trådløst nettverk
- autentisering
- tilgangskontroll
- kryptering

Men selv om man oppretter en sikker sone, må virksomheten fortsatt ha noen generelle datasikkerhetstiltak for alle systemer. Eksempler er innlogging med passord, brannmur og antivirusprogram.

Det er lettere å få aksept fra brukerne for strenge sikkerhetstiltak for sensitive data når det er tydelig at det er nødvendig med sikkerhet.

Vurdere risiko og konsekvenser

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vurdere risiko og konsekvenser (113837)

For å vurdere behovet for sikkerhetstiltak kan du gjennomføre en risiko-/konsekvensanalyse.

En risiko-/konsekvensanalyse kan gjøres både for virksomhetens IKT-systemer som helhet og for enkeltsystemer. Analysen starter med å besvare spørsmålet:

Hva kan gå galt?

For hvert punkt du lister opp som svar på dette spørsmålet, må du svare på tre nye spørsmål:

1. Hva blir konsekvensen hvis det som kan gå galt, faktisk går galt?
2. Hvor stor er sjansen for at det kommer til å skje?
3. Hvilke tiltak må gjennomføres for å forhindre at det går galt – eller for å begrense skaden hvis det går galt?

Med utgangspunkt i svarene kan du vurdere konsekvensene og sjansen for at noe går galt, opp mot kostnadene ved å gjennomføre sikkerhetstiltakene. Da har du et grunnlag for å bestemme hvor omfattende tiltak som må iverksettes.

Hvis for eksempel konsekvensene er små og det er liten sjanse for at noe kommer til å skje, vil behovet for sikkerhetstiltak også være lite.

Hvis konsekvensene derimot er kritiske for virksomheten, vil behovet for sikkerhetstiltak også være stort – selv om sjansen for at noe kommer til å skje, fortsatt er liten.

En brann som ødelegger alle tjenere slik at alle programmer og data går tapt, er for eksempel lite sannsynlig. Men hvis det skulle skje, kan det i verste fall føre til at virksomheten må opphøre, at den går konkurs eller lignende.

Risikodiagram

Som hjelp til vurderingen kan du bruke et risikodiagram. Her er et eksempel på et slikt diagram:

En brann i et kontorbygg kan få store konsekvenser dersom ikke tjenere og annen IKT-infrastruktur er godt nok sikret.
Fotograf: Pontus Lundahl

Vær oppmerksom på at når det gjelder registrering av **personinformasjon** er det satt minimumskrav til sikkerhet i loven om personregister. Disse kravene kan ikke fravikes selv om man vurderer både konsekvensene og sjansene for at noe kan gå galt, som lave.

Lenke

Kunnskapssenteret – Risikoanalyse/-matriser

Sikkerhetsrisiko:					
	Konsekvenser				
Sannsynlighet	Minimale	Små	Middels store	Store	Kritiske
Svært sannsynlig					

Sannsynlig					
Lite sannsynlig					
Svært lite sannsynlig					

Risikodiagram. Forfatter: Arne Jansen

I diagrammet angir radene sannsynligheten for at noe kommer til å skje, mens kolonnene viser hvor alvorlige konsekvensene kan bli.

Rutene i diagrammet har en fargekode som viser om graden av risiko er akseptabel, og hvilket nivå av sikkerhet som kreves.

- **GRØNN** = Akseptabel risiko. Krever ikke spesielle sikkerhetstiltak.
- **GUL** = Mulig risiko. Spesielle sikkerhetstiltak bør vurderes.
- **RØD** = Uakseptabel risiko. Krever spesielle sikkerhetstiltak.

Med «spesielle sikkerhetstiltak» menes tiltak som gjøres spesielt for å forhindre eller begrense skaden av den bestemte risikoen.

Hvis konsekvensene av en hendelse er kritiske, vil behovet for sikkerhetstiltak være stort selv om det er liten sjanse for at noe kommer til å gå galt.

Tre typer sikkerhet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Tre typer sikkerhet (113838)

Vi kan dele inn skader og problemer som kan oppstå med IKT-systemer, i tre hovedkategorier med tilhørende sikkerhetstiltak:

- fysisk skade > fysisk sikkerhet
- driftsavbrudd > driftssikkerhet
- tap eller tyveri av data > datasikkerhet

Fysisk sikkerhet er tiltak for å beskytte datautstyr mot fysisk skade. Fysisk skade kan være alt fra brann- og vannskader til hærverk eller tyveri av utstyr.

Driftssikkerhet er tiltak som blir gjort for å hindre at for eksempel et maskinproblem fører til at arbeid eller oppgaver som krever bruk av datamaskiner, blir avbrutt i lengre perioder.

Datasikkerhet, eller informasjonssikkerhet, er tiltak for å beskytte informasjon. Det inkluderer både beskyttelse mot tap av data og mot ulovlig innsyn, misbruk eller tyveri av informasjon.

Hvis det ikke er gjort noe for å begrense skadevirkninger, vil et problem i en kategori ofte forplante seg slik at man også får problemer i de andre kategoriene. For eksempel blir tyveri av en tjener regnet for å være en fysisk skade, men det vil også føre til driftsavbrudd og tap av data hvis man ikke har gjort de nødvendige sikkerhetstiltakene for å forhindre slike konsekvenser.

Vi kan dele inn skader og problemer som kan oppstå med IKT-systemer, i tre hovedkategorier med tilhørende sikkerhetstiltak – fysisk skade, driftsavbrudd og tap eller tyveri av data.

Fysisk sikkerhet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Fysisk sikkerhet (113840)

Fysisk sikkerhet er tiltak for å beskytte datautstyr mot fysisk skade. Det kan være alt fra brann- og vannskader til hærverk eller tyveri av utstyr.

En datamaskin er gjerne et fristende bytte for en innbruddstyv. Men vanligvis skaper ikke tyveri av en vanlig pc så store problemer for virksomheten at pc-er bør tyverisikres på andre måter enn annet utstyr som har tilsvarende verdi.

Når et pc-tyveri skaper problemer, skyldes det som regel at man mister viktige data, eller at data kommer på avveier. Men da er det ikke først og fremst den fysiske sikkerheten, men datasikkerheten som har sviktet.

Det stiller seg imidlertid annerledes med maskiner som har spesielle oppgaver, og som ikke kan erstattes på en enkel måte hvis de blir skadet. Eksempler på slike er nettverkstjenere. For slike maskiner vil kravene til fysisk sikring være større fordi konsekvensene av en skade eller et tyveri vil være langt mer alvorlige for virksomheten.

Det er derfor vanlig å plassere tjenere i rom som kan sikres på forsvarlig måte mot uautorisert adgang eller innbrudd. Det kan også være aktuelt å ha egen brannalarm og automatisk utstyr for brannslokking. Da blir det brukt gass, siden vann, skum eller pulver kan skade utstyret like mye som en brann.

Større virksomheter har gjerne egne datarom hvor man også kan kontrollere temperaturen og begrense statisk elektrisitet.

For bærbare pc-er eller utstyr som står utsatt til for tyveri, kan det være aktuelt å bruke en pc-lås.

Brent pc.

Fotograf: Pyroclastichawk

Pc-lås.

Fotograf: Florian Boyd

Lenke

Fysisk sikring av datarom

Når et pc-tyveri skaper problemer, skyldes det som regel at man mister viktige data, eller at data kommer på avveier.

Driftssikkerhet

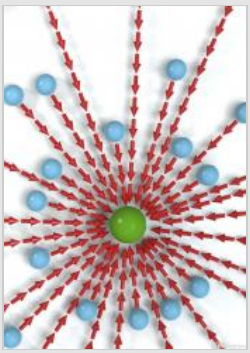
Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Driftssikkerhet (113842)

Driftssikkerhet er tiltak som blir gjort for å hindre at for eksempel et maskinproblem fører til at arbeid eller oppgaver som krever bruk av datamaskiner, blir avbrutt i lengre perioder.

Et driftsavbrudd er normalt ikke noe stort problem for virksomheten når det rammer en enkelt pc. Men hvis nettverkstjeneren plutselig stanser, vil det føre til at alle som bruker programmer og data som ligger på tjeneren, heller ikke kan bruke sine maskiner. Et langvarig driftsavbrudd kan derfor bli svært kostbart hvis virksomheten er avhengig av datasystemer for å fungere.

Vanlige årsaker til driftsavbrudd er harddiskkrasj, strømbrudd, brudd på nettverkskabel eller feil i sentrale maskin- eller nettverkskomponenter. Avbrudd kan også forårsakes av datavirus eller feil i programmer.

På Internett kan hackere forårsake driftsavbrudd ved å blokkere tilgangen til virksomhetens nettsider – såkalte DOS-angrep (Denial of Service).



Denial of Service-angrep blir ofte gjort ved å «bombardere» for eksempel en nettside med så mye trafikk at siden ikke klare å respondere.

Et langvarig driftsavbrudd kan bli svært kostbart hvis virksomheten er avhengig av datasystemer for å fungere.

Feiltolerante systemer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Feiltolerante systemer (113844)

På grunn av de alvorlige konsekvensene et langvarig driftsavbrudd kan få, legger maskin- og programvareprodusentene ned et stort arbeid i å konstruere såkalte feiltolerante systemer.

Et feiltolerant system innebærer at utstyret er konstruert slik at en enkelt feil ikke skal kunne slå ut hele systemet. På engelsk kalles dette gjerne for «No Single Point of Failure».

Den mest effektive måten å sikre seg mot driftsavbrudd på er å ha reserveutstyr som står klart til å ta over hvis det skulle oppstå en feil på hovedutstyret. I et nettverk er det mulig å sette opp en reservetjener som står som en nøyaktig kopi av hovedtjeneren. Hvis hovedmaskinen feiler, overtar reserven. En slik reservemaskin kalles for en speiltjener (mirrorserver) fordi den – for alle praktiske formål – er som et speilbilde av hovedmaskinen.

Enkelte maskinprodusenter bygger også maskiner som er spesielt konstruerte med tanke på å unngå driftsstans. Slike maskiner inkluderer gjerne et dobbelt sett av alle sentrale komponenter, i tillegg til innebygd avbruddsfri strømforsyning og RAID-diskløsninger. Hvis en komponent skulle svikte, vil reservekomponenten straks overta, og driften opprettholdes.

Ulempen med duplisering av utstyr er at det fort blir svært kostbart. I virksomheter hvor en driftsstans ikke har umiddelbare alvorlige konsekvenser, velger man derfor ofte rimeligere alternativer.

En vanlig pc kan for eksempel settes opp som reservetjener, slik at de viktigste funksjonene kan opprettholdes inntil man kan skaffe en ny maskin. De fleste maskinleverandører tilbyr også serviceavtaler som garanterer at en maskinfeil vil bli reparert eller at en byttemaskin er på plass i løpet av et visst antall timer fra feilen varsles.

For å unngå langvarig driftsavbrudd kan det være lurt å sette opp en speiltjener.
Fotograf: Science Photo Library

Lenke

Feiltoleranse – Store norske leksikon

Et feiltolerant system innebærer at utstyret er konstruert slik at en enkelt feil ikke skal kunne slå ut hele systemet.

RAID-løsninger

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
RAID-løsninger (113846)

Harddisker og andre datalagringssystemer er et svakt ledd i de fleste IKT-systemer. Siden harddisker er mekaniske, kan det oppstå fysiske skader som kan gjøre at det ikke er mulig å lese eller skrive data til dem. Populært blir dette kalt harddiskkrasj.

RAID er betegnelsen på en teknologi for feiltolerant datalagring som fordeler og dupliserer data over flere harddisker. Dette blir gjort på en slik måte at selv om én disk feiler, vil ingen data gå tapt, og det vil fortsatt være mulig å lese og skrive data til disksystemet.

RAID er en forkortelse for Redundant Array of Inexpensive Disks (overflødig matrise av billige disker). Tidligere var også betegnelsen Redundant Array of Independent Disks (overflødig matrise av uavhengige disker) i bruk.

Hvordan fungerer RAID?

I praksis fungerer RAID på den måten at flere harddisker kobles sammen slik at resultatet blir økt hastighet og bedre driftssikkerhet. Det er definert en rekke ulike RAID-nivåer fra 0 til 6, men det er bare enkelte av dem som blir brukt i praksis.

RAID 0 er bare en metode for å øke dataoverføringshastigheten for harddisker som er koblet i serie. RAID 0 kalles også for «diskstriping» og har ingen feiltoleranse.

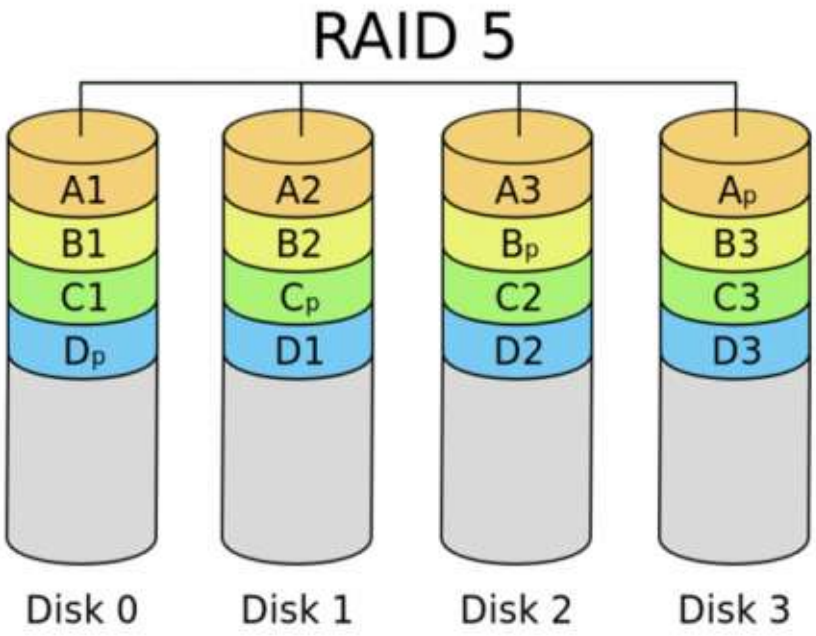
RAID 1 er **diskduplisering** (diskspeiling) hvor alt skrives på to harddisker samtidig. Hvis den ene harddisken krasjer, vil alle data fortsatt være intakte på den andre.

De fleste RAID-løsningene er basert på RAID 5 eller 6. I RAID 5 brukes tre eller flere harddisker som er koblet sammen, og alle data stripes over alle diskene på bitnivå. Det betyr at hvert tegn som skal lagres, blir delt opp og spredd på flere disker. Deretter beregner systemet en kontrollsum for dataene som også lagres på en av diskene. Dette kalles for **paritetsberegning**, og det er denne kontrollsummen som sørger for feiltoleranse.

Hvis en harddisk krasjer, kan den tapte informasjonen regenereres ved hjelp av kontrollsummene på de andre diskene. I et system som er i bruk, blir dette gjort fortløpende slik at brukerne ikke engang merker at en harddisk ikke lenger fungerer. Det gjør det i tillegg mulig å skifte en defekt harddisk uten at man må stanse systemet.

Illustrasjonen under viser et eksempel på RAID 5 med fire harddisker. En serie data, kalt A, blir delt opp og spredd på hver av de tre første diskene (A1, A2 og A3). På den siste disken skrives paritetsberegning for dataserien (Ap). Det samme gjentas for neste dataserie (B), men nå skrives data på de to første og den siste disken, mens paritetsberegningen skrives til den tredje disken. Slik fortsetter systemet å spre paritetsberegningen ut over alle diskene.

Dette blir gjort for å unngå at paritetsberegningen for alle data skal bli lagret på en enkelt disk. Det har ingen betydning for feiltoleransen hvis en disk krasjer, men det er raskere å regenerere data når det oppstår en diskkrasj, hvis paritetsberegningen er spredt på alle diskene, for da mister man færre data.



Fotograf: Colin M.L. Burnett

Hvis nå for eksempel den første disken krasjer, mister vi dataene A1, B1 og C1. Men ved hjelp av kontrollsummen Ap på den siste disken og de uskadde dataene A2 og A3, kan systemet regne ut hva som var lagret i A1. Det samme gjelder for dataseriene B og C. For dataserien D er det ikke nødvendig å regenerere noen data siden det bare var kontrollsummen for denne serien som var lagret på den første disken.

RAID 6 fungerer på samme måte som RAID 5, med det tillegg at det lagres to kontrollsummer på ulike harddisker slik at to disker kan feile samtidig uten at noen data går tapt.

Lenke

RAID – Wikipedia

RAID innebærer at flere harddisker kobles sammen på en slik måte at resultatet blir økt hastighet og bedre driftssikkerhet.

Avbruddsfri strømforsyning

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Avbruddsfri strømforsyning (113847)

Siden datamaskiner er avhengige av strøm for å fungere, er dette et svakt punkt sett fra et driftssikkerhetsståsted.

Et uventet strømbrudd fører ikke bare til at maskinen stanser – man risikerer også å miste data som ennå ikke er lagret på harddisken. Enkelte programmer kan også få problemer hvis maskinen blir slått av uten at programmet først er avsluttet på en ordentlig måte.

En løsning på problemet er å installere en enhet for avbruddsfri strømforsyning (Uninteruptable Power Supply, forkortet UPS). En avbruddsfri strømforsyning er et batteri som kobles mellom datamaskinen og strømtilførselen. Datamaskinen vil da få strøm fra batteriet, som igjen lades kontinuerlig fra den vanlige strømtilførselen. Hvis strømmen plutselig skulle bli borte, vil datamaskinen fortsatt få strøm fra batteriet, og når strømmen kommer tilbake, vil batteriet bli ladet opp igjen.

Hvis strømbruddet blir langvarig, får man fortsatt mulighet til å lagre data og avslutte alle programmer før batteriet er tømt. Det finnes programvare som kan gjøre dette automatisk når batteriet begynner å gå tomt for strøm.

Avbruddsfrie strømforsyninger løser også et annet problem. Mange av komponentene i datamaskinen er følsomme for variasjoner i strømstyrken, og et plutselig strømsjokk, for eksempel ved lynnedslag, kan ødelegge maskinen. En avbruddsfri strømforsyning vil sørge for at datamaskinen hele tiden får jevn strømstyrke og spenning.

Et lynnedslag kan slå ut og ødelegge en datamaskin.
Fotograf: Sven Grundmann

Et uventet strømbrudd fører ikke bare til at maskinen stanser – man risikerer også å miste data som ennå ikke er fysisk lagret.

Datasikkerhet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datasikkerhet (113848)

Datasikkerhet, eller informasjonssikkerhet, er tiltak for å beskytte informasjon. Det inkluderer både beskyttelse mot tap av data og mot ulovlig innsyn, misbruk eller tyveri av informasjon.

Her skal vi først og fremst se på tiltak mot tap av data. Tiltak mot ulovlig innsyn, misbruk eller tyveri av informasjon er behandlet i det neste kompetansemålet «Aktivisere, vurdere og dokumentere sikkerhetsmekanismer for å forebygge og varsle forsøk på sikkerhetsbrudd».

Tap av data kan skje på mange måter og vil før eller senere ramme alle datamaskinbrukere. Den vanligste årsaken er rene uhell som enten skyldes uforsiktighet eller manglende kunnskaper hos brukeren. Filer blir slettet ved en feiltakelse, programmer blir avsluttet uten at arbeidet er lagret, eller eksisterende data blir overskrevet. Alt er vanlige feil, men i de fleste tilfellene er ikke skaden større enn at konsekvensene begrenser seg til litt irritasjon og ekstraarbeid.

Verre er det med ødelagte lagringsmedia eller harddiskkrasj. Hvis det ikke finnes en kopi av dataene, kan skaden være uopprettelig.

Regelmessig systematisk **sikkerhetskopiering** er den eneste fullgode måten å sikre seg mot tap av data på. Det koster ofte langt mer å rekonstruere den informasjonen som ligger lagret i en datamaskin, enn å erstatte selve maskinen. Sikkerhetskopier er derfor en svært rimelig forsikring. En harddisk som krasjer, eller en maskin som bryter sammen eller blir stjålet, er vanligvis enkel å erstatte, men data som ligger lagret i maskinen, kan representere flere års arbeid og i enkelte tilfeller til og med være uerstattelige for virksomheten.

Legg merke til at feiltolerante harddiskssystemer som RAID først og fremst sørger for driftssikkerhet. De kan ikke erstatte sikkerhetskopier som beskyttelse mot datatap. Selv om RAID sørger for at data ikke går tapt ved en harddiskkrasj, gir det ingen beskyttelse mot filer som slettes ved et uhell, eller hvis alle data går tapt i for eksempel en brann.

Gode rutiner for sikkerhetskopiering er derfor det viktigste tiltaket du kan gjøre for å ivareta datasikkerheten.

Regelmessig systematisk sikkerhetskopiering er den eneste fullgode måten å sikre seg mot tap av data på.

Sikkerhetskopiering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikkerhetskopiering (113849)

For å sikre at data ikke går tapt, må det finnes gode rutiner for sikkerhetskopiering – og det må være en som er ansvarlig for at rutinen blir fulgt.

Tap av data kan skje på mange ulike måter:

- feil på lagringsmedia – for eksempel harddiskkrasj
- fysisk skade på lagringsmedia – for eksempel brann- eller vannskade
- tyveri av maskin eller lagringsmedia
- sletting ved et uhell, uforsiktighet eller manglende kunnskaper – for eksempel en bruker som sletter en fil i stedet for å flytte den
- bevisst sletting
- datavirus

Husker du dette om sikkerhetskopiering?

For å kunne beskytte mot alle typer datatap må vi stille noen krav til sikkerhetskopiene og rutinene for sikkerhetskopiering.

- Man må ta sikkerhetskopier regelmessig.
- Man må ha sikkerhetskopier som gjør det mulig å gjenopprette gamle data tilbake i tid.
- Man må ikke oppbevare sikkerhetskopiene sammen med originaldataene.
- Man må ha et system som gjør det mulig å finne tilbake til gamle sikkerhetskopier.

I tillegg er det også nødvendig med en rutine for å kopiere data fra en sikkerhetskopi tilbake (restore).

Det er også viktig å huske på at det kan være andre enheter enn pc-er og nettverkstjenere som har data som bør sikres – for eksempel nettbrett eller smarttelefoner. Slike enheter krever ofte egne rutiner for sikkerhetskopiering.

Oppbevaring av sikkerhetskopier

Sikkerhetskopier må oppbevares på en måte som gjør at de ikke går tapt samtidig som originaldataene, for eksempel ved en brann. I praksis betyr det at sikkerhetskopiene må fysisk lagres på et annet sted, og da helst i et annet bygg, enn originaldataene.

Når det ikke er mulig, kan man bruke et brannsikkert skap som plasseres et annet sted i det samme bygget. Det finnes også brannsikre kofferter og andre løsninger for trygg oppbevaring.

Det kan være fort gjort å slette informasjon ved en feil.

Hvilke rutiner bør bedriften ha for å sikre data på de ansattes smart-telefoner? Fotograf: Erlend Aas

Tap av data kan skje på mange ulike måter, og rutinene for sikkerhetskopiering må beskytte mot alle.

Utstyr for sikkerhetskopiering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Utstyr for sikkerhetskopiering (113855)

Man kan i utgangspunktet ta sikkerhetskopier til alle typer lagringsmedier, og det finnes i tillegg nettbaserte tjenester. Men ikke alle lagringsmedier er like godt egnet for sikkerhetskopiering.

CD eller DVD

CD- eller DVD-plater kan brukes til enkel sikkerhetskopiering. Platene er rimelige og enkle å oppbevare, men lagringskapasiteten er begrenset. CD eller DVD kan likevel være en grei løsning for frittstående maskiner eller i situasjoner hvor datamengdene er små.

Minnepinner

Minnepinner kan brukes til å kopiere viktige data, men de er lite egnet for regelmessig sikkerhetskopiering. Kapasiteten er større enn for CD- og DVD-plater, men den er fortsatt begrenset. Minnepinne kan likevel være et alternativ for frittstående maskiner.

Ekstern harddisk

En ekstern harddisk har like god kapasitet som en intern harddisk, og overføringen av data er rask og enkel. Mange eksterne harddisker kommer også med egne programmer for sikkerhetskopiering. Ulempen er at det fort blir kostbart når man må ta vare på mange sikkerhetskopier for å kunne gjenopprette filer tilbake i tid.

Datakassetter/bånd

Datakassetter/bånd er som regel det beste alternativet for sikkerhetskopiering av tjenere i nettverk. Båndene er spesielt laget for sikkerhetskopiering, de har stor lagringskapasitet og er enkle å oppbevare.

Datakassetter/bånd krever imidlertid en egen båndstasjon (streamer) og programvare for sikkerhetskopiering.

Nettbasert sikkerhetskopiering

En DVD-plate.

Fotograf: Science Photo Library

En minnepinne.

Fotograf: Henrik Björnsson

En ekstern harddisk.

Fotograf: Sebastian Vandrey

Flere leverandører tilbyr nettbasert (online) sikkerhetskopiering via Internett, og noen programvareprodusenter tilbyr også nettbasert sikkerhetskopiering som en integrert del av programmene sine.

Ved nettbasert sikkerhetskopiering sendes en kopi av dataene som skal kopieres, til en tilbyder som lagrer dataene i et datasenter.

En slik løsning krever ikke noe annet enn en internettilgang, og man betaler for den mengden data man lagrer. Men nettbasert sikkerhetskopiering kan ha noen andre sikkerhetsutfordringer – blant annet fordi konfidensielle data regelmessig må sendes via Internett. Vi må derfor kunne stole på at tilbyderen beskytter dataene tilstrekkelig mot tyveri og uautorisert innsyn, og at de ikke går tapt hvis det skjer en ulykke hos tilbyderen.

Magnetiske databånd for datalagring.

Datalagring i «skyen».

Begrenset varighet

Varigheten av digitale lagringsmedier som CD-er, DVD-er, harddisker, minnepinner og datakassetter er begrenset, og etter en tid vil de enten bli uleselige eller miste evnen til å holde på data. De fleste produsenter anbefaler derfor at data leses over på nye media innen 5–10 år.

Lenke

Slik sikrer du filene dine – Artikkel fra Teknofil.no

Hvor lenge holder digitale lagringsmedier? – Artikkel fra Illustrert Vitenskap

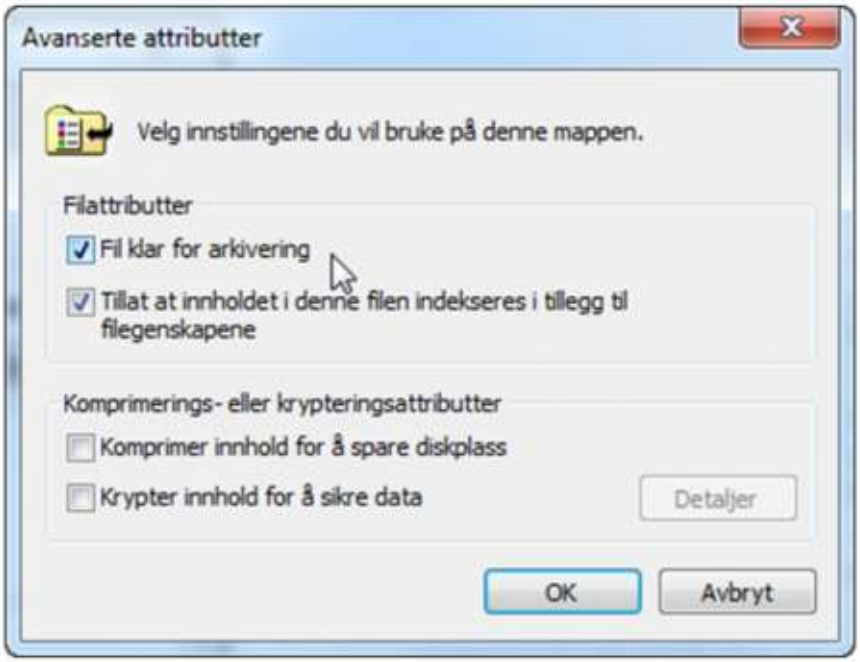
Datakassetter/bånd er som regel det beste alternativet for sikkerhetskopiering av tjenere i nettverk.

Differensiell og inkrementell sikkerhetskopiering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Differensiell og inkrementell sikkerhetskopiering (113858)

I filsystemet er det bygget inn funksjoner spesielt med tanke på rutiner for sikkerhetskopiering. Blant annet er det mulig å kun ta sikkerhetskopi av filer som har endret seg siden forrige kopiering.

Alle filer og mapper har noen egenskaper som kalles for **attributter**. I Windows kan du se attributtene for en fil eller mappe ved å høyreklikke på den og velge egenskaper. Nederst i dialogboksen med generelle egenskaper vises attributtene for skrivebeskyttelse og skjult samt en knapp for å vise avanserte attributter.



Dialogboks for avanserte attributter.

Opphavsmann: Microsoft

Det interessante filattributtet for sikkerhetskopiering kalles for arkiv-attributtet og vises i dialogboksen som «**Fil klar for arkivering**». Programmer for sikkerhetskopiering bruker dette attributtet når de skal avgjøre om en fil er endret siden forrige kopiering.

Hvis arkiv-attributtet er slått på («Fil klar for arkivering» er haket av), er filen endret siden forrige sikkerhetskopiering. Hvis arkiv-attributtet er slått av, er det motsatt.

Windows slår på arkiv-attributtet når en fil blir lagret. Du kan kontrollere dette selv ved først å slå av arkiv-attributtet for en fil. Deretter åpner du filen, gjør en endring, og lagrer den. Nå vil det stå en hake ved «Fil klar for arkivering» igjen.

Programmer for sikkerhetskopiering bruker dette attributtet ved å slå det av for alle filer det tar en kopi av. Når du senere ønsker å ta en ny sikkerhetskopi, kan du be om at programmet bare tar kopi av de filene som er endret siden sist. Dette vil da være alle filer hvor arkiv-attributtet er blitt slått på fordi de er blitt lagret på nytt.

Fordelen med å bare ta kopi av de filene som er endret, er at sikkerhetskopieringen går mye raskere og kopien tar vesentlig mindre plass.

For å kunne holde orden på hva sikkerhetskopieringsprogrammet skal ta kopi av, har ulike typer av sikkerhetskopier forskjellig betegnelse.

En normal eller **full sikkerhetskopiering** er det vi kan kalle for en vanlig sikkerhetskopi. Det vil si at programmet tar kopi av alle mapper og filer uavhengig av om arkiv-attributtet er slått av eller på fra før. Merk at programmet vil slå av arkiv-attributtet for alle filene når kopieringen er utført.

Når vi starter sikkerhetskopiering, må vi alltid begynne med en normal sikkerhetskopi, men etter dette kan du godt benytte et av de to andre alternativene, kalt **differensiell sikkerhetskopiering** og **inkrementell sikkerhetskopiering**.

Begge tar bare kopi av filer som har arkiv-attributtet slått på – altså bare filer som er endret eller er nye siden forrige sikkerhetskopi.

Forskjellen på differensiell og inkrementell består i hva de gjør med arkiv-attributtet. Differensiell sikkerhetskopiering vil la arkiv-attributtet stå urørt, mens inkrementell vil slå det av på samme måte som en normal eller full sikkerhetskopiering.

Type sikkerhetskopi	**Tar kopi av**	**Arkiv-attributt**
Normal	alle filer uavhengig av hva arkiv-attributtet er satt til	slår av arkiv-attributtet
Inkrementell	kun filer hvor arkiv-attributtet er slått på	slår av arkiv-attributtet
Differensiell	kun filer hvor arkiv-attributtet er slått på	endrer ikke arkiv-attributtet

Figur: Typer sikkerhetskopiering. Forfatter: Arne Jansen

Sikkerhetskopiering med rotasjon av lagringsmedier

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikkerhetskopiering med rotasjon av lagringsmedier (113860)

De ulike typene sikkerhetskopiering kan kombineres for å lage en effektiv sikkerhetskopieringsrutine med rotasjon av lagringsmedier (backup-rotasjon).

En tabell for rotasjon av lagringsmedier kan se slik ut:

Kopieringstidspunkt	Kopitype	Bånd
lørdag 01.00	full	uke 1
tirsdag 01.00	inkrementell	dag 1
onsdag 01.00	inkrementell	dag 2
torsdag 01.0	inkrementell	dag 3
fredag 01.00	inkrementell	dag 4

Figur: Forslag til rotasjon – sikkerhetskopiering. Av Arne Jansen

Kopieringen er automatisert og starter automatisk kl. 01.00 om natten når det er liten eller ingen aktivitet. Man begynner med en fullstendig sikkerhetskopi av alle data. Denne lagres på et bånd som blir kalt «uke 1».

Det tar normalt både en del tid og en del plass å kjøre en full kopiering. Etter neste arbeidsdag er det tvilsomt at alle filene er blitt endret, så da er det ingen grunn til å ta kopi av alle filene igjen. Man kan da ta en inkrementell sikkerhetskopi, som bare vil ta med de filene som er blitt brukt eller opprettet etter den normale sikkerhetskopien. Den nye sikkerhetskopien tar derfor mye mindre plass og går langt raskere.

Før kopien kjøres, må man bytte ut båndet med ett nytt som blir kalt for «dag 1», og man flytter «uke 1»-båndet til en sikker oppbevaring.

Slik fortsetter man med inkrementelle sikkerhetskopier på nye bånd (dag 2–4) fram til neste gang det er tid for en full sikkerhetskopiering igjen – etter en uke.

Da starter rotasjonen på nytt med en ny fullstendig sikkerhetskopi, og man bruker da enda et nytt bånd som blir kalt for «uke 2». Når man skal gjøre de inkrementelle sikkerhetskopiene etter hver arbeidsdag, bruker man dagsbåndene på nytt.

Slik fortsetter man, og på slutten av måneden er det ett ukesbånd for hver av de siste fire ukene. Det siste båndet legges til side og kalles for «måned 1» eller navnet på måneden. Så starter rotasjonen på nytt med ukesbånd 1 og de fire dagsbåndene, og så tar man ut det siste av ukesbåndene hver måned.

Etter ett år har man følgende:

- kopi av alle data og endringer som er gjort den siste uken (ukesbåndet og de fire dagsbåndene)
- kopi av alle data slik de var i slutten av hver uke for de siste fire ukene (ukesbåndene)
- kopi av alle data slik de var i slutten av hver måned for de siste tolv månedene (månedsbåndene)

Totalt er det brukt 19 bånd, og hvis det er behov for det, kan man også legge det siste båndet i hvert år til side før rotasjonen starter igjen.

Dette kan virke unødvendig tungvint, men vi kan se på noen eksempler som viser hvorfor et slikt system er fornuftig.

- Hvis noen har opprettet en ny fil på en tirsdag og ved et uhell sletter den dagen etter, vil filen kunne hentes fram igjen fra kopien som ble tatt natt til onsdag («dag 1»-båndet).
- Hvis noen opprettet en fil for en uke siden og ved et uhell sletter den i dag, vil ikke filen finnes på noen av dagsbåndene – men den kan hentes fram igjen fra den siste ukeskopien.
- Hvis noen oppretter en fil i februar, sletter den ved et uhell i mars, og oppdager det først i mai, vil filen kunne hentes fram fra månedsbåndet fra februar.

Muligheten for å kunne gå tilbake i tid kan også være avgjørende hvis man blir rammet av et datavirus som det tar tid før man oppdager. Det kan føre til at man må gjenopprette data fra uken eller måneden før systemet ble infisert.

Et alternativ vil selvsagt være å bruke et nytt bånd til hver sikkerhetskopi, men det blir unødvendig kostbart.

Du finner et eksempel på en rutine for sikkerhetskopiering som benytter en rotasjon som beskrevet over, i kompetansemålet «Dokumentere og gjøre tilgjengelig løsninger på problemer» i Bruker- og driftsstøtte.

Lenke

Sikkerhetskopiering – Veiledning fra NorSIS

Sikker sletting av data

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikker sletting av data (113869)

Vi er vanligvis mest opptatt av å unngå å miste data, men i noen tilfeller er utfordringen det motsatte. Vi har behov for å slette data på en slik måte at det ikke er mulig for uvedkommende å gjenopprette dem.

Behovet for å slette data permanent oppstår gjerne når en maskin skal kasseres, gis bort, selges eller må sendes til service.

Innholdet i filer som er slettet på vanlig måte, kan forholdsvis enkelt hentes frem igjen. Du er helt sikkert kjent med at når du sletter en fil på vanlig måte, legges den først i papirkurven slik at det er mulig å angre.

Men selv om du tømmer papirkurven, blir ikke filen slettet fysisk. Det eneste som skjer, er at den plassen filen opptar på lagringsmediet, markeres som ledig – slik at filen ikke lenger vises i utforskeren eller papirkurven. Selve innholdet i filen blir liggende urørt helt til nye data skrives på det området hvor den gamle filen ligger.

Det finnes en rekke programmer som kan hente fram igjen slettede filer, for eksempel Piriform Recuva.

Formatering av en harddisk er ikke mye bedre. På samme måte som vanlig sletting vil ikke det som ligger lagret på harddisken, bli fysisk fjernet eller overskrevet. Filene vises bare ikke i utforskeren lenger. Det kan sammenlignes med å rive ut innholdsfortegnelsen i en bok.

Den enkleste måten å sikre at data ikke kan gjenopprettes på, er ødelegge lagringsmediet fysisk, for eksempel ved å bruke en slegge på en harddisk. Ulempen er selvsagt at disken blir ubrukelig. Dette er derfor bare et alternativ for maskiner som skal kasseres.

Den sikreste måten å unngå at data kan gjenopprettes på, er å ødelegge pc-en fysisk. Det finnes imidlertid metoder for å hente ut data fra harddisker som er fysisk ødelagte, men det krever spesialkompetanse.
Fotograf: Jens Sølvberg

En annen metode for å slette data er å avmagnetisere lagringsmediet. Harddisker og magnetbånd lagrer data magnetisk, og ved å kjøre dem gjennom en avmagnetiseringsenhet, også kalt en degausser, blir alle data fysisk slettet. Ulempen er også her at mange typer lagringsmedium ikke kan brukes igjen etter at de er blitt avmagnetisert.

For å fjerne data permanent fra et lagringsmedium på en måte som ikke skader mediet, må dataene **overskrives** med nye data. Helst mange ganger. Det finnes mange programmer som gjør nettopp dette. Et eksempel er Eraser.

Videoer
IBAS
How to Destroy a Hard Drive and Data

Lenker
Sikker sletting – Artikkel fra DinSide.no
Degausser.com

Ved vanlig sletting eller formatering vil ikke det som ligger lagret på harddisken, bli fysisk fjernet eller overskrevet.

IKT og HMS

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
IKT og HMS (113874)

Arbeidsmiljøloven har strenge regler for å sikre at arbeidstakere ikke blir skadet eller syke av jobben. Arbeidstilsynet har også laget en egen forskrift for arbeid ved dataskjerm.

Kravene til arbeidsmiljø i arbeidsmiljøloven gjelder også for dem som arbeider med IKT, men Direktoratet for arbeidstilsynet har i tillegg laget en egen forskrift for arbeid ved dataskjerm. (Forskrift av 15.12.1994 nr. 1259)

Forskriften stiller krav til

- tilrettelegging og organisering av dataskjermarbeidsplasser
- utstyr
- fysisk miljø
- oppfølging av arbeidstakernes syn
- opplæring og informasjon

Stillesittende arbeid foran en dataskjerm kan være er en medvirkende årsak til helseplager. Spesielt er belastningen på synet stor.

Belastningen vil være ekstra stor dersom arbeidstakeren har nedsatt funksjonsevne, for eksempel har redusert syn, lese- og skrivevansker eller har sykdom eller skade som gir nedsatt muskelkraft eller utholdenhet. I slike tilfeller vil det være behov for spesielle tilpasninger av arbeidsplassen.

Forskriften om arbeid ved dataskjerm er beregnet på alle arbeidstakere. Men som IKT-servicemedarbeider må du også være oppmerksom på skader som kan oppstå hvis du må løfte eller flytte på datautstyr.

Unngå å løfte eller bære tunge maskiner, skrivere eller annet utstyr. Bruk en tralle eller lignende for å transportere utstyr. Når du må løfte noe – bruk riktig løfteteknikk. Se løfteteknikk.

Riktig arbeidsstilling er viktig foran en pc.

Riktig løfteteknikk.

Lenker

Veiledning om arbeid ved dataskjerm

Forskrift for arbeid ved dataskjerm

Direktoratet for arbeidstilsynet har laget en egen forskrift for arbeid ved dataskjerm.

Krav til det fysiske arbeidsmiljøet og universell
utforming av IKT er også omtalt i Bruker- og driftsstøtte under kompetansemålet «Gi råd
i henhold til gjeldende regelverk ved anskaffelse, bruk og utvikling av IKT-systemer».

Krav til utstyr for en dataarbeidsplass

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Krav til utstyr for en dataarbeidsplass (113875)

§ 10-22 i forskriften om utførelse av arbeid stiller spesifikke krav til arbeidsplassen og IKT-utstyr. I tillegg har Arbeidstilsynet gitt en del anbefalinger for gode dataskjermarbeidsplasser.

Skjerm

- Skjermen bør være en LCD- eller plasmaskjerm av god kvalitet.
- Skjermbildet skal være rolig, uten flimmer eller andre forstyrrelser.
- Det må være mulig å justere skrifttype, skriftstørrelse og farger.
- Tegnene på skjermen må være tydelige, og det skal være tilstrekkelig avstand mellom tegn og linjer.
- Det skal være mulig å justere lysstyrke og kontrast.
- Skjermen skal kunne vinkles, roteres og høydereguleres.
- Skjermen skal ikke gi reflekser eller gjenskinn som kan medføre ubehag.
- Midten av skjermbildet bør være i 15–30 grader under øyets horisontallinje
- Synsavstanden bør være 50–70 centimeter.

Tastatur

- Tastaturet skal være utformet så lavt som mulig og bør kunne skråstilles.
- Tastaturet skal være atskilt fra skjermen.
- Tastaturet skal ha en matt overflate for å unngå reflekser.
- Tastaturet bør ha følbar trykkmotstand og lavt støynivå.
- Symbolene på tastene skal være tydelige fra den normale arbeidsstillingen.
- Det skal være tilstrekkelig plass foran tastaturet til å støtte underarmer og hender.

Legg spesielt merke til kravet om at tastaturet skal være atskilt fra skjermen. Dette er fordi brukeren skal kunne bruke tastaturet uten å bli trøtt i hender, armer, skuldre eller nakke.

Forskriften gjelder ikke for bærbare pc-er som brukes i korte perioder, men hvis brukeren skal bruke en bærbar pc regelmessig, tilsvarende en vanlig datamaskin, skal kravene i forskriften oppfylles. Det betyr at brukeren skal ha eksternt tastatur, skjerm og mus.

Mus og pekeutstyr

- Utstyret skal ha en form som passer i hånden.
- Utstyret skal kunne brukes med både høyre og venstre hånd.
- Utstyret bør ha en tynn og myk ledning, eventuelt være trådløst.

Arbeidstilsynet anbefaler at virksomheten skaffer ulike typer mus og pekeutstyr, slik at brukerne kan prøve ut hvilket utstyr de foretrekker.

Arbeidsbord

- Arbeidsbordet må være stort nok til at det er god plass til utstyr og underarmsstøtte, samt plass til bruk av mus foran tastaturet.
- Arbeidsbordet skal ha en matt overflate.
- Arbeidsbordet bør kunne heves og senkes.

Arbeidsstol

En dataskjerm skal blant annet kunne reguleres i høyden.
Fotograf: Mike Schröder

Mus og tastatur skal være behagelige å bruke.
Fotograf: Lise Åserud

Det er viktig med en god kontorstol som det er mulig å regulere.
Fotograf: Corbis

- Arbeidsstolen skal være stødig og ha fem hjul.
- Stolen skal gi bevegelsesfrihet og en bekvem arbeidsstilling.
- Stolsetet skal ha regulerbar høyde og bør også kunne reguleres i dybden.
- Stolryggen skal kunne reguleres i høyden og skal kunne skråstilles.
- En fotstøtte skal stilles til rådighet for dem som ønsker det.
- Ved behov skal underarmstøtte kunne påmonteres.

Vær spesielt oppmerksom på at bærbare pc-er som brukes regelmessig, skal ha eksternt tastatur, mus og skjerm.

Databriller

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Databriller (113880)

Arbeidstakere som får problemer med synet på grunn av arbeid ved dataskjermen, har krav på synsundersøkelse og databrille.

Arbeid ved dataskjerm setter store krav til øynene fordi synsavstanden er kort og synsfeltet er lite. Øyet er ikke spesielt egnet for å se på nært hold, og mye arbeid ved skjerm kan overbelaste de små øyemusklene. Resultatet kan bli nærsynthet, synstretthet, sviende eller kløende øyne, svimmelhet og hodepine.

For å avhjelpe dette står det i forskriften om arbeid ved dataskjerm at arbeidstakere som jobber ved dataskjerm, skal få tilbud om øyeundersøkelse og synsprøve

- før de begynner arbeid ved dataskjermen
- om nødvendig med jevne mellomrom i tiden deretter
- dersom de får synsproblemer som kan skyldes arbeidet ved dataskjermen

Hvis synsundersøkelsen viser at det er behov for synskorrigerende hjelpemidler utover vanlige briller eller linser som arbeidstakeren allerede bruker, har arbeidstakeren krav på en databrille.

Databrille er et samlebegrep for brillekorreksjoner som er spesielt tilpasset arbeidstakere som arbeider ved dataskjerm. Det vil som oftest være en enstyrkebrille, men det finnes også progressive/multifokale briller som er gode til skjermbruk. Vanlige progressive briller for daglig bruk regnes imidlertid ikke som databriller.

Øynene er utsatt for store belastninger når man arbeider foran en skjerm hele dagen.
Fotograf: Jann Lipka

Arbeidstakere som har behov for synskorrigerende hjelpemidler på grunn av arbeid ved dataskjerm, har krav på en databrille.

Lenke

Databriller – Informasjon fra Arbeidstilsynet

Datautstyr og miljø

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datautstyr og miljø (113882)

Selv om datamaskiner kanskje ikke hører til de verste forurensningskildene, er det etter hvert blitt så mange av dem at du må være oppmerksom på at de også kan utgjøre en miljøtrussel.

For det første benytter datamaskiner strøm. På mange arbeidsplasser lar de ansatte datamaskinen stå på til og med når de går hjem, for å slippe å måtte starte den når de kommer neste dag. Dermed blir maskiner stående på om natten, i helger og i ferier. Selv om maskinen går i dvalemodus, trekker den fortsatt strøm.

Det samme gjelder skjermer, skrivere, høyttalere og annet tilkoblet utstyr. For å redusere strømforbruket bør virksomheten ha en regel som sier at utstyret skal slås av når man forlater arbeidsplassen for dagen.

Dette har også et sikkerhetsaspekt. En datamaskin som står pålogget uten at noen er i nærheten, er en sikkerhetsrisiko. Spesielt hvis det er andre som kan ha tilgang til den utenfor arbeidstid.

Resirkulering

Komponentene i datamaskiner og annen elektronikk inneholder tungmetaller som helst ikke skal havne i naturen. Man har derfor begynt å resirkulere komponentene i gamle datamaskiner, og mange leverandører har opprettet egne resirkuleringsprogram.

I Norge har vi også EE-forskriften som stiller krav til mottak, innsamling og gjenvinning av kasserte elektriske og elektroniske produkter. Formålet med forskriften er å redusere de miljøproblemene elektriske og elektroniske produkter forårsaker når de ender som avfall. Forskriften gir produsentene, kommunene og forhandlerne ansvar for retur av EE-avfall.

Andre miljøtiltak

Ikke la pc-en stå på når du ikke bruker den.
Fotograf: Science Photo Library

Resirkulering av gammelt IT-utstyr.

Forsøk å unngå å ta utskrifter om du kan!
Fotograf: Bjørge Stein

Lenke

EE-forskriften

Utskrifter er et annet område hvor det er mulig å være miljøbevisst. Ved å publisere og lese mest mulig dokumentasjon på skjerm unngår man unødvendige utskrifter.

Mange miljøtiltak bidrar også til reduserte kostnader.

Men når noe først må skrives ut, er det også muligheter. Mange skrivere har for eksempel mulighet for tosidig utskrift. Nettverksskrivere er ofte også konfigurert for å skrive ut en ekstra side mellom utskrifter fra ulike brukere. Denne funksjonen kan vanligvis slås av uten at det skaper problemer.

Videre er det mulig å bruke tonerkassetter til laserskrivere og blekkpatroner om igjen ved å fylle på ny toner eller nytt blekk.

I tillegg til å være miljøvennlige gir slike tiltak også reduserte kostnader.

Sikkerhet

Innledning til forebygging av sikkerhetsbrudd

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innledning til forebygging av sikkerhetsbrudd (124727)

Datasikkerhet eller informasjonssikkerhet er tiltak for å beskytte virksomhetens informasjon. Det inkluderer både beskyttelse mot tap av data og mot ulovlig innsyn, misbruk eller tyveri av informasjon.

I 2012 anslo Nasjonal sikkerhetsmyndighet (NSM) at det ble begått nesten 45 000 datakriminelle handlinger i Norge. Disse handlingene førte til at norske virksomheter tapte om lag 20 milliarder kroner. Tallene er ventet å øke i årene fremover, så trusselen er reell. Vi må ta sikkerheten på alvor.

En datakriminell fremstilles gjerne som en fremmed som tar seg inn i datamaskinen via Internett for å stjele eller ødelegge informasjon. De fleste datatyverier i vanlige virksomheter gjøres imidlertid ikke av fremmede, men av personer som har lovlig tilgang til systemet. Det skaper ekstra utfordringer. Det er ofte enklere å beskytte seg mot eksterne angrep enn mot personer som har fysisk tilgang til systemet.

De fleste nettverkssystemer har muligheter for automatisk overvåking av hvem som bruker systemet, og hva de gjør med det. Men slik overvåking kan være problematisk når det gjelder egne brukere og ansatte, fordi det fort kan komme i konflikt med de lovene som gjelder for personvern og arbeidsmiljø. (*Ref. Bruker og driftsstøtte, kompetansemål 1 «Behandle fortrolige opplysninger på en etisk forsvarlig måte innenfor rammene av gjeldende regelverk.")*

Et annet problem med datatyverier er at forbrytelsen kan være vanskelig å oppdage fordi det er umulig å se at data er blitt kopiert. Hvis tyven ikke legger igjen andre spor, blir det kanskje aldri oppdaget.

De datatyveriene som ofte er vanskeligst å oppdage, utføres av personer med legitim adgang til datasystemene.
Fotograf: Damian Dovarganes

Dersom sikkerhetstiltakene blir for strenge, kan de hindre de ansatte i å utføre jobben sin.
Fotograf: Science Photo Library

For en systemansvarlig er tiltak for å forebygge sikkerhetsbrudd derfor ofte en balansegang. Hvis sikkerheten blir for streng og kontrolltiltakene for detaljerte, er det en risiko for at systemene blir for tungvinte å bruke og at man kommer i konflikt med personvernet og arbeidsmiljøvernlovgivningen. Men hvis sikkerheten ikke er streng nok, risikerer man at sensitiv informasjon kommer på avveier eller blir misbrukt.

Norsk senter for informasjonssikring (NorSIS) har laget ei håndbok for informasjonssikkerhet som skal fungere som en standard for informasjonssikkerhet i små og mellomstore virksomheter, og som kan brukes for lage et eget sikkerhetsregelverk.

- **Lenke**: Håndbok for informasjonssikkerhet
- **Lenke**: Datakrim for 20 milliarder kroner. Artikkel fra NRK.
- **Lenke**: NRK Brennpunkt om datakriminalitet

Datatyverier kan være vanskelige å oppdage fordi det er umulig å se at data er blitt kopiert.

Holde Windows pc-er oppdatert

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Holde Windows pc-er oppdatert (124734)

Windows kan ha svakheter som kriminelle kan utnytte for å få tilgang til maskinen. Når slike svakheter oppdages, sender Microsoft ut en oppdatering som retter problemet gjennom en funksjon som kalles Windows Update.

Svakheter i operativsystemer, nettlesere og annen programvare kan utnyttes av personer som ønsker å få tilgang til data som ligger på maskinen, til å installere uønskede programmer eller til å overta kontrollen over maskinen. Slike svakheter kalles gjerne for sikkerhetshull, og programvareprodusentene kommer derfor med regelmessige oppdateringer som «tetter hullene» etter hvert som de oppdages.

Alle oppdateringer har ikke nødvendigvis med sikkerhet å gjøre. Det kan også være retting av feil, støtte for nytt tilleggsutstyr eller forbedringer av eksisterende funksjoner. Men det er uansett svært viktig å holde operativsystemet oppdatert.

Windows har en innebygget funksjon kalt Windows Update som automatisk laster ned og installerer oppdateringer via Internett. Denne funksjonen bør være slått på.

Les mer om Windows Update her.

Windows 8 er den nyeste versjonen av Microsoft. Den ble lansert oktober 2012.
Fotograf: Henrik Montgomery

Konfigurere Windows Update

Du åpner Windows Update fra kontrollpanelet eller ved å klikke på start-knappen og skrive «Windows Update» i søkefeltet.

Fra «Windows Update»-vinduet kan du

- søke etter nye oppdateringer
- endre innstillingene for hvordan oppdateringer skal lastes ned og installeres
- se en logg over hvilke oppdateringer som er installert tidligere
- gjenopprette eventuelle skjulte oppdateringer

Søke etter nye oppdateringer

Hvis du er usikker på om en maskin er oppdatert, kan du be Windows om å se etter nye oppdateringer. Dette bør du gjøre hvis

- Windows akkurat er blitt installert eller installert på nytt på maskinen
- maskinen ikke har vært i bruk på en stund
- maskinen ikke har vært koblet til Internett på en stund
- automatiske oppdateringer har vært slått av
- hvis du er usikker på om maskinen er oppdatert

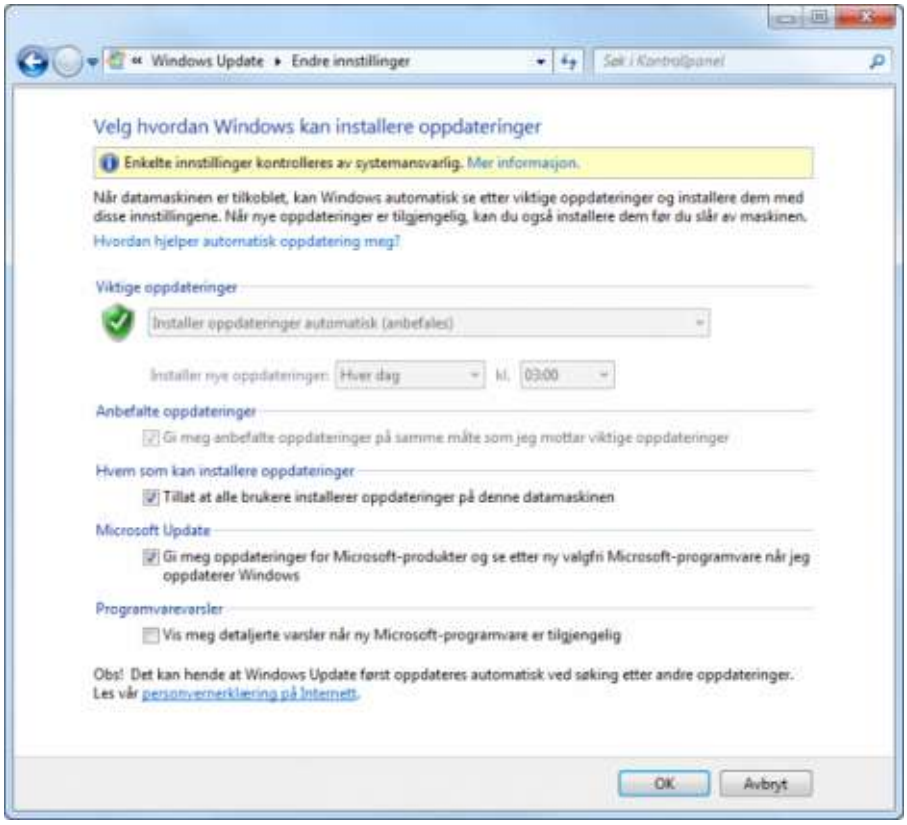
Windows Update leter etter oppdateringer til maskinen.

Opphavsmann: Microsoft

Endre innstillinger for Windows Update

Når datamaskinen er tilkoblet Internett, kan Windows automatisk se etter nye oppdateringer og installere dem. Hvis det ikke er spesielle grunner for det motsatte, bør denne funksjonen alltid være slått på.

For maskiner som står i et nettverk, kan systemansvarlig låse oppdateringsfunksjonen slik at den ikke kan endres av brukerne. I illustrasjonen under ser du hvordan det ser ut. Valgene under «Viktige oppdateringer» og «Anbefalte oppdateringer» er grå, og teksten «Enkelte innstillinger kontrolleres av systemansvarlig» vises øverst. Dermed er det ingen fare for at en bruker uforvarende slår av den automatiske oppdateringen.



Velg hvordan Windows kan installere oppdateringer.

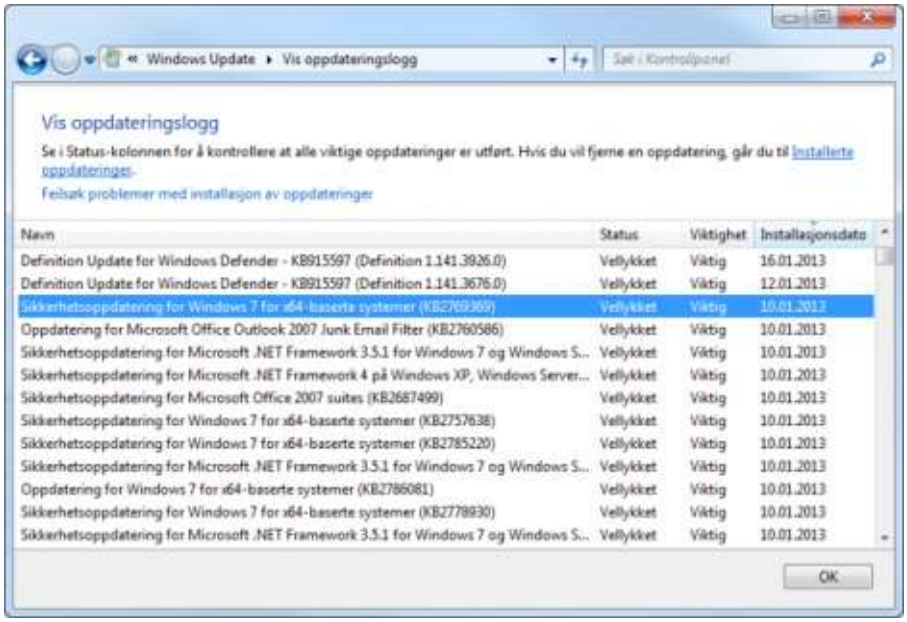
Opphavsmann: Microsoft

De fleste oppdateringer krever administrativ tilgang til Windows for å kunne installeres. Ved å huke av for valget «**Tillat at alle brukere installerer oppdateringer på denne datamaskinen**» vil nye oppdateringer bli installert selv om brukeren ikke har slike rettigheter.

I tillegg til oppdateringer for Windows kan vi også la Update søke etter oppdateringer for andre Microsoft-programmer, som for eksempel Microsoft Office, ved å huke av for valget «**Microsoft Update**».

Oppdateringsloggen

Du kan sjekke hvilke oppdateringer som er installert på maskinen ved å velge «**Vis oppdateringslogg**».



Vis oppdateringslogg i Windows.

Opphavsmann: Microsoft

I tillegg til å vise hvilke oppdateringer som er installert, viser loggen også om installasjonen var vellykket eller mislykket, hvor viktig den er, og datoen da den ble installert.

Det kommer nye oppdateringer hver måned, så hvis loggen viser at det ikke er installert noen oppdateringer på flere måneder, eller at noen av oppdateringene er mislykket, er det et tegn på at noe er galt.

Skjulte oppdateringer

Skjulte oppdateringer er oppdateringer som er blitt lastet ned, men som du har bedt om at Windows Update ikke skal varsle deg om eller ikke installere automatisk. Hvis Windows Update er konfigurert til å installere oppdateringer automatisk, skal denne lista være tom.

- **Lenke**: Slik holder du din Windows PC oppdatert

Hvis ikke det er spesielle grunner for det motsatte, bør Windows Update alltid være konfigurert for å laste ned og installere oppdateringer automatisk.

Holde Apple Mac-maskiner oppdaterte

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Holde Apple Mac-maskiner oppdaterte (124742)

På samme måte som Windows må også Apples Mac OS oppdateres regelmessig for at sikkerheten skal være ivaretatt.

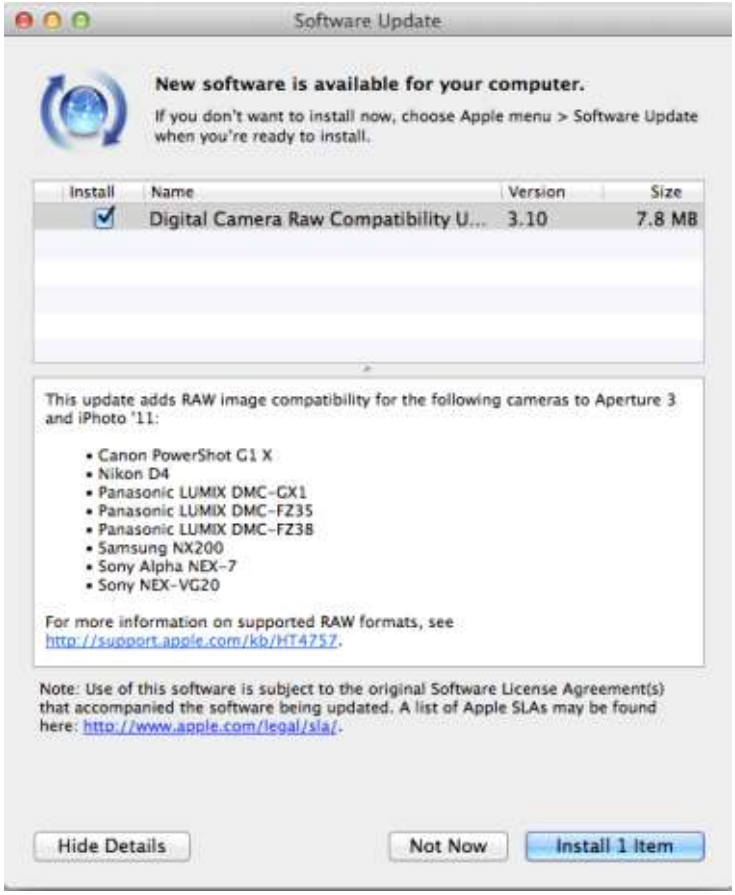
Som for Windows har ikke nødvendigvis alle oppdateringer av Mac OS med sikkerhet å gjøre, men maskinen bør uansett holdes oppdatert for å unngå feil og problemer.

Fra versjon 10.5 søker Mac OS automatisk etter nye oppdateringer når maskinen er koblet til Internett, men som standard blir du først spurt om du vil installere oppdateringen.

Oppdateringer av programvare for Mac IOS.

Opphavsmann: Apple Inc.

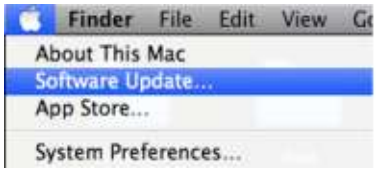
Hvis du er usikker på hva oppdateringen gjelder, kan du klikke på Show Details. Da vises en oversikt over hvilket eller hvilke programmer som vil bli oppdatert, og en forklaring på hva oppdateringen gjør.



Ny programvare tilgjengelig for Mac IOS.

Opphavsmann: Apple Inc.

Hvis du velger å utsette installasjon av en oppdatering, kan du installere den seinere ved å velge Software Update (Programvareoppdatering) fra Apple-menyen.



Konfigurere Apple Software Update.

Opphavsmann: Apple Inc.

Du åpner Apple Software Update ved å klikke på Software Update-ikonet i System Preferences.

Programvareoppdatering i Mac IOS.

Opphavsmann: Apple Inc.

Du kan velge om maskinen skal se etter nye oppdateringer daglig, ukentlig eller månedlig, og om oppdateringene skal lastes ned automatisk. Hvis maskinen er koblet til Internett og brukes regelmessig, bør du minimum velge ukentlig og helst daglig.

Legg merke til at selv om oppdateringer lastes ned automatisk, må du fortsatt bekrefte at du vil installere dem. Av den grunn bør en maskin som ikke skal brukes på en stund, ikke stå koblet til Internett påslått.

App Store-programmer

Software Update oppdaterer alle programmer som hører til Mac OS, men den sjekker ikke oppdateringer for programmer som er kjøpt fra Mac App Store. For å oppdatere disse programmene må du åpne App Store og klikke på «Updates» i menyen øverst i vinduet. Da viser en oversikt over hvilke programmer som har oppdateringer, og du kan velge hvilke du vil installere.

- **Lenke**: Slik holder du din Mac oppdatert
- **Lenke:** Get Software Updates for Your Mac

Selv om Mac OS automatisk laster ned nye oppdateringer, blir de ikke installert før du godkjenner det.

Oppdatering av andre programmer

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Oppdatering av andre programmer (124747)

I tillegg til operativsystemet er det ofte mange andre programmer på en datamaskin som også må oppdateres, og som ikke er inkludert i de automatiske oppdateringene.

For Apple Mac blir for eksempel ikke programmer som er kjøpt via App Store automatisk oppdatert, og Windows Update sjekker ikke oppdateringer for programmer som kommer fra andre produsenter enn Microsoft.

Noen programmer sjekker automatisk – eller spør deg om du ønsker å sjekke om det finnes oppdateringer – når det startes. For andre må du selv sjekke om det er kommet oppdateringer.

I en del tilfeller kan du også velge om oppdateringer skal gjøres automatisk. For noen typer programmer er dette fornuftig. For eksempel bør antivirusprogrammer, nettlesere og programkomponenter som Java og Flash alltid være oppdatert med nyeste versjon.

Men automatiske oppdateringer har også ulemper. Det kan føre til at maskinen går tregere, og at oppstart tar lengre tid. Automatiske oppdateringer kan også skape problemer hvis maskinen er koblet til en internettforbindelse som har begrenset kapasitet.

Oppdateringsplan

Det er derfor fornuftig å lage en oppdateringsplan for den programvaren virksomheten bruker. En god løsning er å dele programmer i tre kategorier:

- programmer som krever automatisk oppdatering
- programmer som bør oppdateres regelmessig
- programmer som ikke krever oppdatering

Programmer som krever automatisk oppdatering, er typisk antivirusprogrammer, operativsystemer, nettlesere og andre programmer som er kritiske for sikkerheten eller spesielt utsatte.

Antivirusprogrammene på en pc bør alltid være oppdaterte.
Fotograf: Science Photo Library

E-post-programmer og andre kontorpakke-programmer bør oppdateres regelmessig.
Fotograf: Trond J. Strøm

Programvare som bør oppdateres regelmessig, er alle programmer hvor det ikke er kritisk for sikkerheten å sjekke om det er kommet oppdateringer hver gang maskinen startes eller hver gang programmet brukes, men som likevel bør oppdateres regelmessig for å få med feilrettinger og nye funksjoner. Dette gjelder de fleste vanlige brukerprogrammer som for eksempel Office-pakker.

Lag en plan over hvilke programmer som må oppdateres, og når det bør skje.
Fotograf: Somos Images

Programvare som ikke krever oppdatering, er ofte spesialprogrammer eller programmer som ikke kommuniserer via Internett. For slike programmer kommer det vanligvis heller ikke sikkerhetsoppdateringer, og eventuelle oppdateringer gjøres gjerne i forbindelse med nye versjoner.

Når du har identifisert hvilke behov for oppdatering ulike programmer har, må du konfigurere de programmene som krever automatisk oppdatering, for dette. I planen bør det stå hvilke programmer dette gjelder, og hvor ofte du skal kontrollere at alle oppdateringer blir installert. For maskiner som står som servere, bør dette helst gjøres ukentlig, mens det for brukermaskiner kan være tilstrekkelig med månedlig eller kvartalsvis kontroll.

For programmer som ikke krever regelmessig oppdatering, lager du en plan for hvor ofte du skal sjekke om det er kommet oppdateringer. Det kan variere for ulike programmer, så det bør være mulig å skrive inn i planen når siste oppdatering ble gjort.

Til sist bør planen inneholde en oversikt over når du skal sjekke om det er kommet nye versjoner av programmer som ikke krever oppdatering.

Fornye gamle programmer

Det er viktig å være klar over at produsenten før eller seinere stanser oppdatering av gamle programversjoner. Microsoft annonserte for eksempel at kundestøtten for Windows XP avsluttes den 8. april 2014. Etter denne datoen kommer det ikke flere sikkerhetsoppdateringer, og maskiner som bruker dette operativsystemet, må enten kasseres eller oppgraderes med et nyere operativsystem hvis sikkerheten skal ivaretas.

Dette er vanligvis ikke noe problem, siden de fleste maskiner blir skiftet ut før programmene blir så gamle at oppdateringer stanses. Men i noen tilfeller brukes maskiner til dedikerte oppgaver som ikke krever at de oppgraderes, for eksempel i prosessindustrien, der den eneste oppgaven til en maskin kan være å styre en produksjonsmaskin, eller på et lager, der maskinen ikke gjør noe annet enn å motta og skrive ut pakkelister.

Hvis slike maskiner har en kobling mot Internett, må de skiftes ut eller oppgraderes hvis programprodusenten stanser sikkerhetsoppdateringer.

Du bør lage en oppdateringsplan for den programvaren virksomheten bruker.

Passord

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Passord (124751)

Den enkleste måten å beskytte data mot ulovlig innsyn på er passordbeskyttelse. Enkle og gode passordrutiner er derfor vesentlig for virksomheten.

Passord kan legges på flere nivåer. Vi kan ha brukerpassord på hver enkelt maskin, påloggingspassord for å få tilgang til data som ligger på nettverksservere, og noen programmer åpner for individuell passordbeskyttelse av enkeltfiler.

Maskinpassord

Muligheten for maskinpassord varierer, men på de fleste maskiner, nettbrett og smarttelefoner er det mulig å sette et passord eller en kode for å låse opp maskinen. Slike passord bør vi bruke på alt mobilt utstyr som vi tar med på reiser eller andre steder utenfor virksomheten, men det er vanligvis ikke nødvendig for maskiner som står fast i et nettverk.

Påloggingspassord

For maskiner i et nettverk er påloggingspassordet den fremste beskyttelsen for å hindre at uvedkommende kan bruke maskinen.

I Windows har brukernavnet og påloggingspassordet flere funksjoner. For det første bestemmer det hvilken brukerprofil Windows skal hente opp. Ulike brukerprofiler kan ha ulike tilganger og rettigheter til systemet, slik at det er mulig å sette grenser for hva en bruker skal ha lov til å gjøre på maskinen.

Profiler kan for eksempel brukes for å hindre at brukere installerer programmer, avinstallerer antivirusprogram, slår av automatiske oppdateringer eller endrer andre innstillinger på maskinen.

iPad med maskinpassord – slik mange mobile enheter har.
Fotograf: Adrianna Williams

Brukernavn og passord for pålogging.
Fotograf: Corbis

Påloggingspassordet brukes også til å identifisere brukeren i nettverket. På samme måte som for brukerprofilen kan systemansvarlig sette ulike rettigheter og tilganger for hver enkelt brukerkonto i nettverket.

Generelt gjelder regelen om at hver bruker skal ha de tilgangene som er nødvendige for å gjøre jobben sin, men heller ikke flere.

I tillegg til at brukeren må identifisere seg, må også maskinen være registrert i nettverket. Nettverk deles inn i domener, og både brukeren og maskinen må være meldt inn som medlemmer i domenet for å få tilgang til ressurser i nettverket. Dette hindrer at personer som eventuelt har fått tak i et brukernavn og passord, skal kunne logge seg inn uten fysisk å sitte ved en maskin som er meldt inn i nettverket.

Filsystembeskyttelse

Filsystemet er den delen av operativsystemet som holder orden på hvor alle filer og programmer ligger på harddisken. I nyere filsystem er det mulig å sette begrensninger for hvem som har lov til å åpne ulike filer og mapper. Det gjør at vi kan gi ulike tilganger til filer og dokumenter hvis flere bruker den samme maskinen eller har tilgang til de samme mappene på en server.

Programpassord og dokumentpassord

Til sist er det mulig å ha passord for å starte bestemte programmer eller åpne filer i programmet. Det er ikke alle programmer som har denne muligheten, men det blir stadig vanligere. I de fleste standardprogrammer som tekstbehandling, regneark og databaser er det mulig å sette passordbeskyttelse på enkeltdokumenter eller enkeltfiler, og i administrative programmer som regnskapssystemer og lignende er det gjerne en passordfunksjon for å kunne bruke programmet. Det samme gjelder nettjenester, hvor e-postadresse ofte brukes som brukernavn i tillegg til passord.

Generelt gjelder regelen om at hver bruker skal ha de tilgangene som er nødvendig for å gjøre jobben sin, men heller ikke flere.

Behandle passord

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Behandle passord (124755)

Et passord gir selvsagt bare sikkerhet så lenge ingen kan gjette eller få tak i det på noen måte. Siden sikkerheten ofte er avhengig av at passord er hemmelige, er det viktig å være bevisst på hvordan passord beskyttes.

Hvordan en angriper forsøker å ta seg forbi en passordbeskyttelse, vil variere etter hva slags passord det er snakk om, men i de fleste tilfeller må den som ønsker å bryte seg inn, på en eller annen måte finne ut hva passordet er. For å gjøre dette kan angriperen

- spørre brukeren hva passordet er
- finne en lapp eller annet hvor brukeren har skrevet ned passordet
- forsøke å gjette passordet
- installere programvare som logger hva brukeren skriver på tastaturet
- bruke programvare som «knekker» passordet

Spørre brukeren om passordet
Det kan høres utrolig ut, men den mest effektive måten å få tak i et passord på er ofte ganske enkelt å spørre brukeren. Typisk vil en angriper utgi seg for å være noen som brukeren tror at han kan stole på. En vanlig framgangsmåte har vært å si at man ringer fra en systemleverandør eller virksomhetens it-avdeling. Den som ringer, vil vanligvis forsøke å gjøre brukeren usikker ved å fortelle at man har oppdaget at noen forsøker å misbruke brukerens konto, at maskinen er infisert av et alvorlig virus eller noe annet som virker skremmende. Hvis den som tar kontakt, virker overbevisende nok, tør ofte ikke brukeren gjøre noe annet enn det vedkommende sier, og da er veien til å spørre om passord kort.

Denne framgangsmåten kalles gjerne for social engineering, og er en mer direkte form for phishing – nettfisking – som vi skal komme tilbake til litt seinere i dette kompetansemålet.

Lenke: Svindlere med falsk PC-hjelp (artikkel på Telenor online)

Den mest effektive måten å få tak i et passord på er å spørre om det. Det skjer ofte over telefonen.
Fotograf: Anders Wiklund

Skriv ned passord

Du har sikkert hørt historier om brukere som skriver passordet sitt på en lapp og fester det på skjermen eller legger det under tastaturet. Selv om det sikkert har forekommet noen slike tilfeller, forstår de fleste at hensikten med passord forsvinner hvis det er så enkelt å finne.

Problemet er likevel at de fleste må forholde seg til en rekke ulike passord og koder, og mange føler at de må skrive dem ned et sted for å være sikre på å huske dem.

I motsetning til det du kanskje har hørt eller lest tidligere, er det ingenting i veien for å gjøre dette, og i mange tilfeller er det faktisk nødvendig. Å skrive ned passord for å huske dem er ikke et problem før noen finner dem.

Mange av passordene vi bruker til daglig, behøver vi imidlertid ikke å taste inn hver gang, for programmene husker dem for oss. Det gjelder for eksempel mange internettjenester, e-post og brukerprogrammer.

Når du først har tastet inn passordet én gang, blir du ikke spurt om det igjen. Men hvis du seinere får en ny maskin eller oppgraderer programvaren, blir du spurt om passordet på nytt.

Da kan det være måneder eller år siden sist du skrev det, og sjansen for at du husker det, er minimal. Faktisk kan de fleste av oss få problemer med å huske et passord vi ellers bruker daglig, hvis det går noen uker uten at vi har bruk for det – for eksempel fordi vi har vært på ferie.

Å skrive ned passord er altså et fornuftig tiltak. Det er hvordan du oppbevarer lappen med passordene, som er vesentlig for sikkerheten. På samme måten som bankkortkoden ikke skal legges sammen med bankkortet, skal ikke passordene finnes i nærheten av datamaskinen. Du vil uansett ikke ha bruk for dem så ofte at de må finnes i umiddelbar nærhet.

En annen side ved passordbehandlingen er de administrative passordene for virksomhetens tenere. Disse passordene må alltid skrives ned slik at det er mulig å få tilgang til systemene hvis det skulle skje en ulykke eller annet som gjør at administrator ikke er tilgjengelig.

Disse passordene krever selvsagt spesiell sikring, og det er anbefalt å skrive dem på et ark som legges i en forseglet konvolutt i for eksempel en safe eller en bankboks. Videre må det selvsagt finnes en rutine som sikrer at man også bytter passordet i konvolutten når passordet i datasystemet blir endret.

Valg av passord

Alle anbefalinger om passord sier at du bør velge et passord som består av usammenhengende bokstaver, tall og tegn. Slike passord er umulige å gjette og vanskeligere å knekke på andre måter. Problemet er bare at de også er vesentlig vanskeligere å huske. Derfor vil de fleste bruke et passord som har betydning for dem, og som er lettere å huske.

Det er gjort flere undersøkelser om hva som er de mest brukte passordene. Passordene i lista under står i tilfeldig rekkefølge:

- «Passord», «Password», «Secret»
- tastaturmønster som «qwerty», rekkefølger som «abc123» eller gjentakelse av det samme tegnet – for eksempel «aaaaa»
- eget navn eller navn på familiemedlem
- fødselsdag eller telefonnummer
- navn på kjæledyr
- navn fra kjente filmer, tv-serier eller romaner
- navn på popstjerner, filmskuespillere, idrettsutøvere, fotballag eller tegneseriefigurer
- navn på øl eller spritmerker
- måneden passordet ble skiftet
- datamaskinmerket

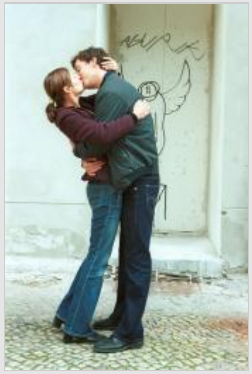
Hvis angriperen vet litt om den personen som eier maskinen, er det altså ikke umulig å gjette passordet. Uansett bør du unngå passord fra lista over siden disse er de første som vil bli forsøkt.

Videre vil mange bruke det samme passordet til flere tjenester, slik at hvis noen får tak i passordet til én tjeneste, får de også tilgang til andre tjenester.

I de fleste serversystemer er det mulig å sette en grense for hvor mange mislykkede innloggingsforsøk man kan gjøre før kontoen blir sperret og må tilbakestilles av en administrator før den kan brukes igjen. Men det gjelder ikke alle internettjenester.

6,5 millioner passord for LinkedIn-brukere lekket ut som følge av hacking i 2012.
Fotograf: Ted Soqui

Administrative passord til en virksomhets servere kan sikres ved for eksempel å legge dem i en konvolutt i en safe.
Fotograf: Berit Roald



Unngå å bruke navn på kjæreste, foreldre, barn eller personer i vennekretsen din som passord.
Fotograf: Frank Rothe

En angriper kan derfor i fred og ro forsøke å gjette en persons passord til en internettjeneste som ikke oppfattes som viktig. Og hvis personen har brukt det samme passordet til andre tjenester, er det fritt fram.

Du bør derfor vurdere hvilken grad av sikkerhet som er nødvendig for ulike tjenester og systemer. Du trenger forskjellige passord for viktige programmer, dokumenter og internettransaksjoner som involverer pengeoverføringer eller overføring av personlig informasjon.

Lag deg en regel som gjør det lettere å huske passordet ditt.

Hva er et godt passord?

- Passordet bør være minst sju tegn langt, men gjerne lengre. Det er først og fremst lengden som gjør et passord vanskelig å knekke.
- Passordet bør være en blanding av store og små bokstaver, tall og spesialtegn. (Store og små bokstaver oppfattes som to ulike tegn av datamaskinen og gjør derfor passordet sterkere.)
- Passordet bør ha minst fem ulike tegn.
- Passordet bør være en tilsynelatende tilfeldig blanding av tegn.
- Passordet bør ikke være et forståelig ord.
- Passordet bør ikke inneholde hele eller deler av påloggingsnavnet ditt.

Bokstavene æ, ø og å kan godt brukes i passord. For alle som ikke bruker norsk tegnsett, vil de bli oppfattet som spesialtegn og gjøre at passordet blir vanskeligere å knekke. Men hvis du reiser utenlands og for eksempel skal sjekke e-posten din via Internett, kan det også bli et problem når du skal skrive inn passordet ditt på et tastatur som ikke har norske tegn.

Hvordan huske passord?

En måte å gjøre passord lettere å huske på uten at det blir lett å gjette, er at du tar utgangspunkt i en setning og så oversetter den til en passende kode som bare du kjenner. For eksempel kan setningen «Jeg har bursdag den 12. mai» kodes om til «Jhbd12.m» ved at du tar den første bokstaven i hvert ord, alle tegn (i dette tilfellet punktum) og tall. Dermed har du et passord som tilfredsstiller alle kriterier for et godt passord, men som likevel er lett å huske fordi du bare trenger å gjenta setningen når du skal skrive passordet.

Når du lager passord på denne måten, så bør du prøve å bruke både tall, tegn og store bokstaver. Det er egentlig ikke så vanskelig. Tall får du ved å bruke klokkeslett, årstall, beløp eller lignende. Store bokstaver er enkelt hvis du tar med en forkortelse, og tegn kan gjerne være punktum, spørsmålstegn, utropstegn, bindestrek og så videre.

Hvis du bruker setninger som har betydning for deg, blir de lette å huske, men umulige for andre å gjette seg fram til.

Passordrutiner i virksomheten

Tidligere var det vanlig å konfigurere servere slik at brukerne ble tvunget til å skifte passord med jevne mellomrom, gjerne hver måned. I dag har de fleste gått bort fra dette fordi det i praksis viser seg at det gir dårligere sikkerhet. Når brukerne stadig må skifte passord, vil de etter hvert velge passord som er enkle å huske og dermed også å gjette – typisk navnet på måneden eller det samme ordet etterfulgt av månedsnummeret. Videre vil flere brukere skrive ned passordet og oppbevare det i nærheten av maskinen. Det er derfor bedre at brukerne har gode passord som de husker, enn å stadig tvinge dem til å forsøke å huske nye passord.

Det gjelder imidlertid ikke for administrative passord til servere. Her bør passordene skiftes regelmessig som en fast rutine.

Lenke: Passordgenerator

Et passord gir bare sikkerhet så lenge ingen kan gjette det eller få tak i det på noen måte.

Datakryptering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datakryptering (124782)

En måte å beskytte data mot innsyn på er å kryptere informasjonen.

Ordet kryptering er avledet av det greske verbet kryptein som betyr «å skjule», og datakryptering innebærer at data gjøres uleselig ved hjelp av en matematisk algoritme. Hensikten er å gjøre informasjon uleselig for alle som ikke har den koden som kan **dekryptere** informasjonen igjen.

Å dekryptere betyr å gjøre kryptert informasjon leselig, og koden som brukes for å kryptere eller dekryptere informasjon, kalles for en krypteringsnøkkel.

Datakryptering brukes på flere måter:

- til å kryptere innholdet av filer når de lagres
- til å kryptere datakommunikasjon
- til å verifisere at en melding ikke er blitt endret etter at den ble sendt
- til å verifisere avsenderen av en melding

Kryptering benyttes også for å autentisere informasjon. For eksempel kan man benytte digitale signaturer for å bekrefte identiteten til en avsender av en e-post.

Ved å kryptere data kan man sikre kommunikasjon over Internett.
Fotograf: Science Photo Library

Symmetrisk og asymmetrisk kryptering

Det er to hovedtyper av kryptering kalt symmetrisk kryptering og asymmetrisk kryptering.

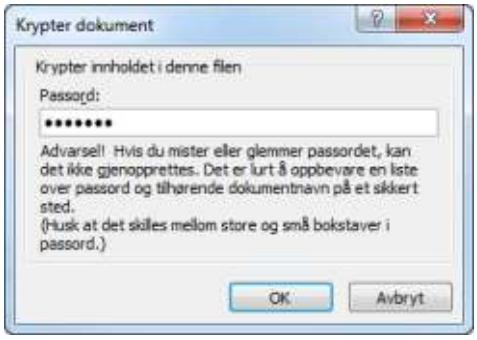
Til kryptering av filer brukes vanligvis symmetrisk kryptering. Symmetrisk kryptering innebærer at den samme krypteringsnøkkelen brukes til både å kryptere og dekryptere informasjonen.

Symmetrisk kryptering er en sikker løsning så lenge nøkkelen (koden) som brukes, kan holdes hemmelig, og den brukes gjerne til kryptering av filer på servere og sikkerhetskopier.

Et eksempel på symmetrisk kryptering er krypteringsfunksjonen i Microsoft Office (se illustrasjoner under).

Krypteringsfunksjonen i Microsoft Office.

Opphavsmann: Microsoft



Krypteringsfunksjonen i Microsoft Office.

Opphavsmann: Microsoft

Men det oppstår et problem med symmetrisk kryptering når data må krypteres ett sted og dekrypteres et annet, fordi nøkkelen da på en eller annen måte må sendes til mottakeren, og det innebærer en sikkerhetsrisiko. I slike situasjoner brukes asymmetrisk kryptering.

Asymmetrisk kryptering er en form for kryptering hvor det lages to krypteringsnøkler som hører sammen. Den ene nøkkelen kalles **offentlig nøkkel**, og den andre kalles **privat nøkkel**.

Den private nøkkelen holdes hemmelig, mens den offentlige nøkkelen kan gis ut til hvem som helst. Den kan for eksempel legges for nedlasting på en nettside.

Data som krypteres med den offentlige nøkkelen, kan bare dekrypteres med den private nøkkelen. En avsender kan derfor bruke den offentlige nøkkelen til å kryptere en melding og sende den til den som har den private nøkkelen, i sikkerhet om at det bare er eieren av den private nøkkelen som kan dekryptere informasjonen igjen.

En melding som krypteres med den private nøkkelen, kan bare dekrypteres med den offentlige nøkkelen. Siden hvem som helst kan få tilgang til den offentlige nøkkelen, er ikke meldinger som krypteres med den private nøkkelen, sikre, men hvis en kryptert melding kan dekrypteres med den offentlige nøkkelen, må den være kryptert med den private nøkkelen. Dermed kan mottakeren være sikker på at meldingen kommer fra eieren av den private nøkkelen, og at den ikke er blitt endret underveis. Slik kryptering kan derfor brukes til å verifisere hvem som er avsenderen, og den benyttes blant annet til digitale signaturer.

Legg merke til at en melding som er kryptert med en av nøklene, ikke kan dekrypteres med den samme nøkkelen. Det er heller ikke mulig avlede den private nøkkelen fra den offentlige nøkkelen.

Asymmetrisk kryptering kan sammenlignes med en dørlås som har to nøkler. Hvis døren låses med den ene nøkkelen, kan den bare åpnes med den andre.

Under ser du et eksempel på en offentlig krypteringsnøkkel, i dette tilfellet Skatteetatens offentlige nøkkel. Virksomheter som skal sende data til skattemyndighetene, kan bruke denne nøkkelen til å kryptere informasjonen før den sendes. Når informasjonen er kryptert med denne nøkkelen, kan den bare dekrypteres med Skatteetatens private nøkkel.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Desktop 9.0.2 (Build 2424)

mQENBEkCJ8kBCADSTmTyAy3ZBKp5uFWMlrz7/Nx5t2qXLH2NZZSG5KZZJjHjWsnD
sp+RVSO32hNysZIE9Kt39xd3hLha7at8b+6FCo+gwbOB9Z0ZOqeXawkZ/o9m+nT7
GQiXRS69t4D8MMW9pP8oTtXI+AxhMgINm0nO24b+G2afUo98aRIF7o5vJXHk12Hh
vyqMiPyNn7tKJ/UfI61ehGROXXTdxQZkCCwcVCjtLKTPgcevbCej3K1CO/P5qKpv
6JWYPYntkoQhkliE+MBzpDV8jBxKkaN5ILjPlKN2UQgFGLMvneCMio8lL6j6IBot
Vp5aut/MrLIAKw4QdtmAVn+PEu9nTLuF5WzNABEBAAG0IEdydW5uZGF0YSA8b3Bl
ckBza2F0dGVldGF0ZW4ubm8+iQFtBBABAgBXBQJJAifJMBSAAAAAACAAB3ByZWZl
cnJlZC1lbWFpbC1lbmNvZGluZ0BwZ3AuY29tcGdwbWltZQcLCQgHAwIKAhkBBRsD
AAAAAxYCAQUeAQAAAAQVCAkKAAoJEFuZVD2zBW5X1cAH/1wmX9btvzgK0sLbNfxW
Czfllbqt T4Up4T/jTymTnaDigRVP7E6PRnB4CwEm9paQ2hGoCQNTIqVwylEMakxV
35sTvlsJoQkGeyxwy+k4u8zx3j1GOIguzmZmSEO1uoLPAMN1arL+1fkJXSaZKYii
tsTfg69diJQgaRrVHMm+NmhMUFruZKGFeucxzKsd8CYr6pn9AAnqGLoLSSkEbYmz
XJJAtdy/6/SLmb424gNQrg4wLKXL9OHffQO+beot07wTZEuOdtjbErorka3sJ3QP
AiGBioqgGneJ4tyDuhTAVBi91g6bOQsmRe2rdVOg/4sRM8wZoTiN0J78OEY2BaGQ
9Fu5AQ0ESQInyQEIAK1YfFdgQo68vJ19YLHaZzkXGbys2LeMIdN2OgCi/PbjZSiu
YeUvJCtbo/7pwsRz/Y/hxg9bMnanY5auIytNH1t2ghxeJNfVFbv002c7XMpthGAe
KWfRHp/vEO4hQ4S0YRzRQjW6zRTdncdJeVg8svC60VDvuRnesvPR0Lg6m1L85jDR
Qkq8fj+JvY3VoJYwXy9dwef3DPppi6GIQdonQFQol+plFeXzbSDOLiiKzecSoe+F
dDboxjx0PlgyRjMX4E+QIw2lETt3rr/TR4z+NqXffHEhgrupT855D4zyT3u2X+2Y
GR6r7Mr1AKHIOAKgh03aM85I+pB1MHG7swGFa1UAEQEAAYkBIgQYAQIADAUCSQIn
yQUbDAAAAAAKCRBbmVQ9swVuV6+8B/9KxJCVLmVdf6AhvtjvWHePkOxr/VvM+Uey
4hVK0mvvtkm8jJjOH+Mi3vzlm0dBfUctNgVU9CLs69H1DjALsegZ8SesJypElVSw
Ny9VqDUtdz0eTjKFEyiOhrAqO1u1MwK/6eyWWT3cvkChYAYGelZZgdJj5sCP6Erc
LAiJz9SFeZvRM8XdbQOSs6qmTjr91PrHt9yYd3gz4OB9tQefnoA9ZfcSO+vwntBI
5gd7kIFZQHnhgb0FqdN4QH+pVihTK97rxjNjkfSyx/fOuo/Bg0YqtsIde0UjzYtK
bphWMl03vGpmfLRnsI6enT62oOzkX4GQhO0EYUfSAUL7oeJWy9x5
=FADg
-----END PGP PUBLIC KEY BLOCK-----
```


Skatteetatens offentlige krypteringsnøkkel.

Asymmetrisk kryptering brukes til all form for sikker kommunikasjon på Internett, for eksempel i nettbanker og e-handelsløsninger.

Den vanligste løsningen er HTTPS, som er den krypterte versjonen av http-protokollen som brukes til å overføre websider.

Lenke: Asymmetrisk kryptering

Lenke: HTTPS

Lenke: Kryptering av mapper og filer

Asymmetrisk kryptering kan sammenlignes med en dørlås som har to nøkler. Hvis døren låses med den ene nøkkelen, kan den bare åpnes med den andre.

Datavirus

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Datavirus (124816)

Datavirus brukes ofte som et samlebegrep for uønskede programmer som på en eller annen måte gjør skade på data eller overtar kontrollen over datamaskinen.

Det finnes flere ulike kategorier av datavirus, men felles for dem er at de spres og installeres på maskinen uten brukerens viten og vilje. En del datavirus utnytter sikkerhetshull i operativsystemer og populære programmer.

Når et datavirus først er kommet inn i en maskin, kan det spre seg videre til andre maskiner i nettverket ved å lese adresselista til brukeren og sende seg selv som e-post til alle som står på den. Dermed ser det ut som om noen du kjenner, har sendt deg en e-post med et vedlegg. Den samme teknikken brukes også i andre programmer som har adresselister og meldingsfunksjoner.

Ormer og trojanske hester

Datavirus deles ofte inn i underkategoriene ormer og trojanske hester. Forskjellen på dem er måten de sprer seg på. En orm har en programkode som gjør at den er i stand til å spre seg selv, mens en trojansk hest er betegnelsen på et virus som skjuler seg inni et annet program og spres når noen laster ned eller kopierer vertsprogrammet.

For å unngå å bli oppdaget før det får spredt seg videre har virus ofte en innebygget forsinkelse som gjør at det ikke skjer noe før på en bestemt dato, etter en bestemt tid eller etter en bestemt handling.

Datavirus kan være ganske harmløse og ikke ha annen funksjon enn å spre seg, men de kan også være svært destruktive og for eksempel slette data, logge hva som gjøres på maskinen, sende data til en angriper eller gi en angriper kontroll over maskinen. Den siste metoden brukes blant annet ved koordinerte angrep mot nettsteder, hvor tusenvis av maskiner deltar i angrepet uten at eieren er klar over det.

Antivirus

For å beskytte mot datavirus må alle maskiner ha oppdatert antivirusprogramvare. De fleste antivirusprogrammer oppdateres daglig for å holde tritt med nye virusvarianter, og leverandørene har et felles varslingssystem for å sikre at nye virus oppdages så raskt som mulig. Oppdateringene gjøres vanligvis automatisk, men du bør likevel sjekke at antivirusprogrammet er oppdatert med jevne mellomrom.

Det finnes en rekke antivirusprogrammer på markedet. De mest kjente er Norman, McAfee, F-Secure og Norton. Disse programmene fungerer som abonnementsordninger, hvor man betaler en årlig avgift til produsenten for regelmessige oppdateringer.

For privatpersoner finnes det også flere gode gratis alternativer tilgjengelig, for eksempel Avast og AVG. Dette er antivirusprogrammer som privatpersoner lovlig kan laste ned fra produsenten og benytte gratis.

En kunstnerisk illustrasjon av datavirus-orm.
Fotograf: Science Photo Library

Kjenner du historien om krigeren Odyssevs og den opprinnelige trojanske hesten? Her kan du lese mer om den.
Fotograf: Science Photo Library

Det er viktig å være klar over at antivirus ikke er noen garanti for at maskinen ikke blir infisert av et datavirus. Oppdateringer til antivirusprogrammer vil alltid komme etter at et nytt virus oppdages. Det er derfor alltid en mulighet for å få et virus som antivirusprogrammet ikke kan oppdage ennå.

Antivirusprogrammet F-Secure.

Opphavsmann: F-Secure

En mann fra Haugesund ble arrestert for datainnbrudd på over hundre datamaskiner. Han skal ha brukt en såkalt trojaner, et datavirus laget for å ta kontroll over datamaskiner. Her er politiadvokat Thor Arne Reitan med den ene av to laptoper som ble brukt.

I mai 2000 ble et stort antall pc-er verden over infisert av den såkalte «love bug»-en.

Fotograf: STR

Råd om datavirusbeskyttelse

- installer alle sikkerhetsoppdateringer for operativsystem og programvare
- ha oppdatert antivirusprogram på alle maskiner
- ikke åpne vedlegg eller klikke på lenker i e-poster eller meldinger hvis du ikke kjenner avsender eller er usikker på om e-posten er ekte

Lenke: Virus på PC-en

Lenke: PST advarer mot minnebrikker

For å beskytte mot datavirus må alle maskiner ha oppdatert antivirusprogramvare.

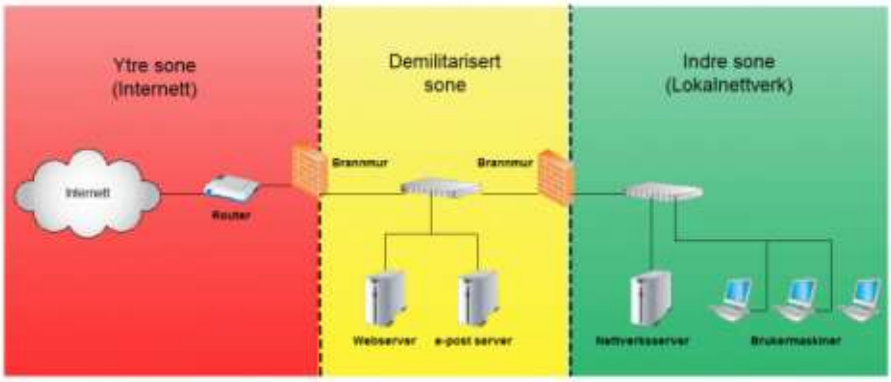
Demilitariserte soner

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Demilitariserte soner (124818)

I IKT-sammenheng brukes benevnelsen demilitarisert sone (DMZ) om en del av en virksomhets nettverk som brukere utenfor virksomheten kan få tilgang til, men som er skilt fra resten av virksomhetens nettverk med en sikkerhetsbarriere.

Hensikten med å opprette en demilitarisert sone er å unngå at noen skal få tilgang til virksomhetens interne nettverk hvis de klarer å bryte seg inn på en maskin som er tilgjengelig fra Internett. Webservere og e-postservere plasseres derfor gjerne i en demilitarisert sone.

Illustrasjonen under viser prinsippet for en demilitarisert sone. Det er ingen direkte kontakt mellom den indre sonen (virksomhetens lokalnettverk) og den ytre sonen (Internett). All trafikk mellom disse må passere gjennom den demilitariserte sonen.



En bedrifts «demilitariserte IT-sone».
Opphavsmann: Arne Jansen

Phishing – nettfisking

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Phishing – nettfisking (124825)

I takt med at teknologien og sikkerheten i datasystemer er blitt bedre, er brukeren blitt det svakeste leddet. Det har gjort phishing – nettfisking – til et stadig større problem.

Phishing er i utgangspunktet hackersjargong for «fisking» (fishing) og henspiller på at man «fisker» etter sensitiv informasjon, passord og lignende. Målet kan også være identitetstyveri.

Den vanligste framgangsmåten er å sende en e-post som ser ut som om den kommer fra en kjent bank, og be om at mottakeren bekrefter informasjon som gjelder konto, kredittkort eller lignende, ved å klikke på en vedlagt lenke. Teksten i e-posten forklarer gjerne at dette er nødvendig av sikkerhetshensyn, eller at kontoen vil bli stengt hvis ikke informasjonen blir bekreftet. Denne informasjonen brukes så til å tappe kontoen for penger.

Svindlerne forsøker å gjøre det hele så troverdig som mulig ved å lage en nettside som ser identisk ut med bankens ekte nettsider, eller ved å kjøre et script som først åpner bankens faktiske nettsider og deretter et mindre vindu over dette hvor man blir bedt om å skrive inn person- og kontoinformasjon.

Andre teknikker inkluderer henvendelser via SMS, nettprat eller telefon.

Thomas Dahl, spesialetterforsker ved Politiets datakrimsenter etterforsker phishing – svindel på Internett. Fotograf: Jan Tomas Espedal

Spearphishing og whaling

Noen metoder for phishing har etter hvert fått egne betegnelser. Spearphishing – spydfisking – er en mer målrettet form for nettfisking som gjerne brukes overfor enkeltpersoner eller virksomheter. Svindleren samler først inn informasjon om virksomheten på forhånd for å kunne gjøre svindelforsøket mer troverdig – for eksempel hvem som jobber i ulike stillinger, kundeforhold, leverandører, samarbeidspartnere og så videre. Denne typen phishing ble tidligere kalt for sosial manipulering (social engineering).

En annen variant er whaling – hvalfangst, hvor svindleren retter seg spesielt mot direktører og personer i lederstillinger.

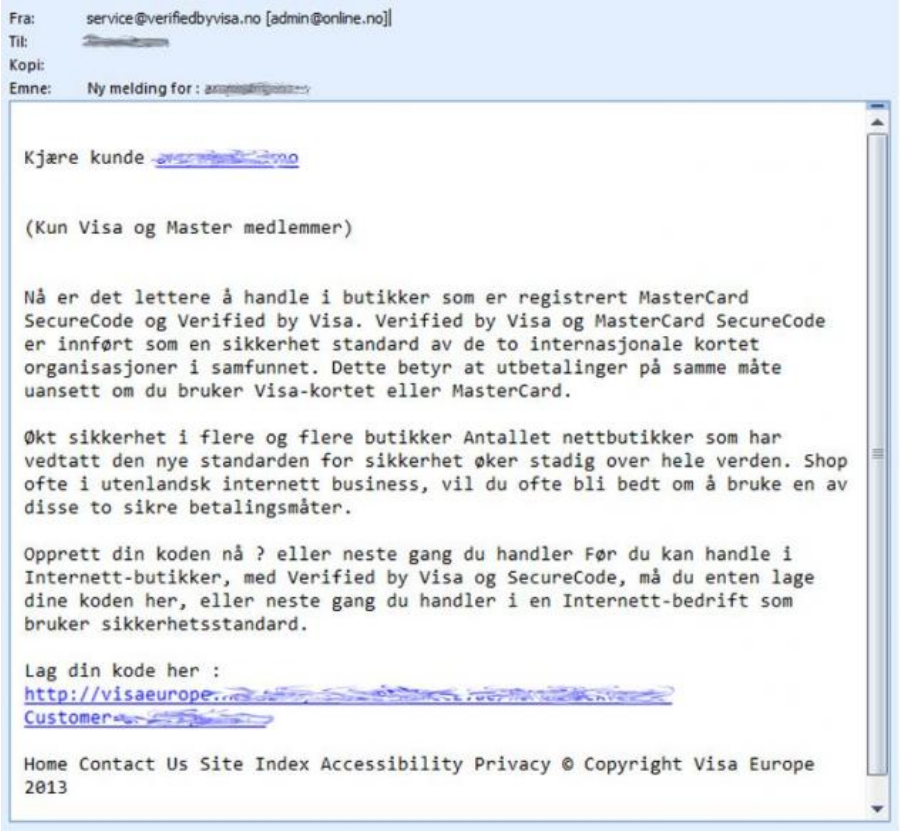
Eksempel på phishing

E-posten under er et typisk eksempel på nettfisking. Personinformasjon og lenker er gjort uleselige.

Avsenderen utgir seg for å være Visa Europe, og innholdet er en oppfordring til å registrere en ny kode for Verified by Visa og MasterCard SecureCode som skal gi deg sikrere og enklere netthandel.

Legg merke til det dårlige språket. Det er et tegn på at avsenderen har begrenset kjennskap til norsk eller har brukt Google Oversetter fra et annet språk. Du bør likevel ikke gå ut fra at du kan avsløre alle phishingforsøk ved å se på språket. Det dukker også opp svindelforsøk på feilfritt norsk.

Uansett sender aldri banker eller kredittinstitusjoner ut e-post hvor de ber kunder om å oppdatere informasjon eller verifisere kontoer. Alle slike meldinger er derfor forsøk på svindel.



Fra: service@verifiedbyvisa.no [admin@online.no]
Til:
Kopi:
Emne: Ny melding for :

Kjære kunde

(Kun Visa og Master medlemmer)

Nå er det lettere å handle i butikker som er registrert MasterCard SecureCode og Verified by Visa. Verified by Visa og MasterCard SecureCode er innført som en sikkerhet standard av de to internasjonale kortet organisasjoner i samfunnet. Dette betyr at utbetalinger på samme måte uansett om du bruker Visa-kortet eller MasterCard.

Økt sikkerhet i flere og flere butikker Antallet nettbutikker som har vedtatt den nye standarden for sikkerhet øker stadig over hele verden. Shop ofte i utenlandsk internett business, vil du ofte bli bedt om å bruke en av disse to sikre betalingsmåter.

Opprett din koden nå ? eller neste gang du handler Før du kan handle i Internett-butikker, med Verified by Visa og SecureCode, må du enten lage dine koden her, eller neste gang du handler i en Internett-bedrift som bruker sikkerhetsstandard.

Lag din kode her :
http://visaeurope...
Customer

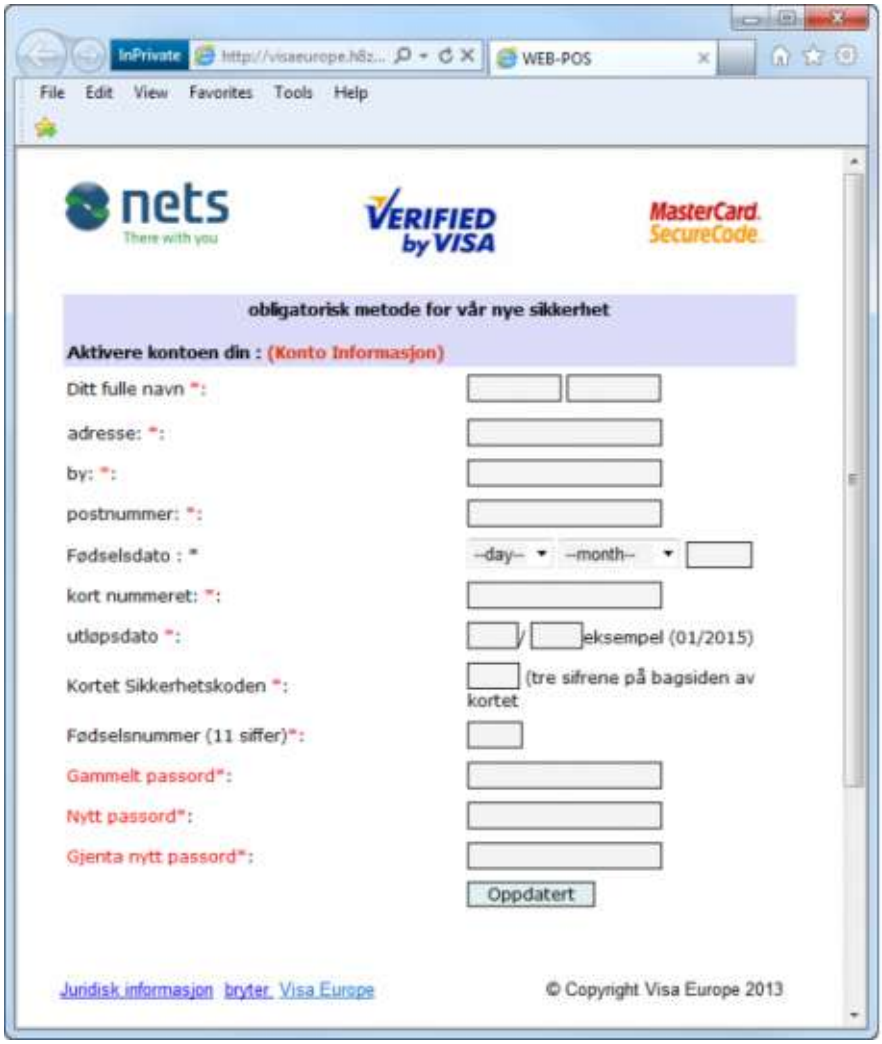
Home Contact Us Site Index Accessibility Privacy © Copyright Visa Europe 2013

Dette brevet er et eksempel på nettfisking – phishing.

Opphavsmann: Arne Jansen

Hvis man klikker på lenken nederst i e-posten, kommer man til nettsiden under.

Merk at du ikke bør klikke på lenker i mistenkelige e-poster. I tillegg til å forsøke å lure deg til å oppgi sensitiv informasjon vil nettsiden som åpnes, ofte også forsøke å installere spionprogramvare på maskinen din. Vi tok derfor ekstra forholdsregler da vi åpnet siden for å kopiere skjermbildet. ***Det korrekte å gjøre er å slette e-posten permanent med én gang.***



Eksempel på forfalsket nettside som er brukt ved phishing – nettfisking.

Opphavsmann: Arne Jansen

Nettsiden ligner på dem som brukes ved sikker betaling på nett, og den ser tilsynelatende legitim ut med logoer fra både Visa og MasterCard. Lenkene i bunnen av siden går også til ekte informasjonssider hos Visa.

Men legg merke til at protokollen som brukes, er http og ikke https. Overføringen er altså ikke kryptert, slik all betalingsinformasjon via Internett alltid skal være.

Videre ber siden om all personinformasjon og kortinformasjon inklusive passord på den samme siden. På ekte betalingssider blir man ikke spurt om all informasjon samtidig, for betalingssystemet må ta kontakt med banken for å verifisere kortet før man får spørsmål om eventuelt passord og kode.

Det er heller ikke noen bank som lar deg bytte passord uten at du først har logget deg inn med det gamle passordet og en gyldig kode.

- **Lenke**:NorSIS artikkel om phishing
- **Lenke**: NorSIS artikkel om sosial manipulering
- **Lenke:** Mobiler sårbare for phishing – artikkel fra PC World Norge

På ekte betalingssider blir man ikke spurt om all informasjon samtidig, for betalingssystemet må ta kontakt med banken for å verifisere kortet før man får spørsmål om eventuelt passord og kode.

Identitetstyveri

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Identitetstyveri (124832)

Når det har vært oppmerksomhet rundt identitetstyveri, har det først og fremst vært fokusert på de problemene det medfører for personer som får sin identitet stjålet. Identitetstyveri er imidlertid også et økende problem for virksomheter.

Når noen stjeler andres identitet, er det vanligvis for å kunne svindle til seg varer eller tjenester. I første omgang skaper dette store problemer for dem som må bevise at de verken har bestilt eller mottatt noen varer, men til slutt er det gjerne virksomhetene som blir sittende igjen med tapet. Dermed blir identitetstyverier også et problem for de virksomhetene som utsettes for svindlere med falsk identitet.

I 2007 startet Norsk senter for informasjonssikring (NorSIS) et prosjekt for å redusere og bremse omfaget av identitetstyverier. På nettsiden idtyveri.info finnes informasjon om identitetstyveri og råd om hvilke forholdsregler både privatpersoner og virksomheter bør ta for å beskytte seg.

For å redusere risikoen for å bli svindlet anbefaler NorSIS at virksomheter bør

- ha en rutine for å sjekke legitimasjon før de inngår avtaler med nye kunder eller kunder de ikke kjenner
- bruke en form for sikker elektronisk ID som signatur fra kunder som bestiller på Internett, for eksempel BankID
- kryptere viktig informasjon som utveksles med kunder via nettsider eller e-post

Virksomheter har også et ansvar for ikke å bidra til å gjøre det enklere å få tilgang til personinformasjon som kan brukes av en identitetstyv. Det betyr at vi må være restriktive med hvilken informasjon vi registrerer om kundene og hvordan vi behandler kundeinformasjon. En virksomhet bør

- ikke samle inn eller registrere mer informasjon enn det som er nødvendig for å ivareta kundeforholdet
- regelmessig slette kundeinformasjon den ikke lenger trenger
- bare gi ansatte som har behov for det, tilgang til kundeinformasjon

Journalist Nedra Pickler i Washington ble utsatt for identitetstyveri og mottok en rekke fakturaer for varer hun ikke hadde bestilt. Fotograf: Kenneth Lambert

Bankenes felles sikkerhetsløsning BankID. Fotograf: Erik Berglund

Virksomhetens identitet kan også misbrukes

Selv om det er mest oppmerksomhet rettet mot de problemene falske kunder skaper, kan en virksomhet også bli direkte utsatt for identitetstyveri.

Virksomheten bør ha regler for hvem som kan publisere informasjon om den på nettsider og sosiale media, og hva det er lov til å publisere, slik at det ikke legges ut informasjon som kan misbrukes til å lage falske kunde- eller bedriftsprofiler.

Et eksempel som det ofte refereres til, er det nystartede firmaet som la ut firmaattesten sin på nettsidene sine. Det tok ikke lang tid før noen skrev ut en kopi som ble brukt til å bestille store mengder varer på kreditt i firmaets navn.

Alle virksomheter må derfor også ha klare regler for hvem som kan opprette kredittavtaler i virksomhetens navn (signaturrett).

- **Lenke**: Idtyveri.info
- **Lenke:** DinSides artikler om identitetstyveri

Virksomheter har også et ansvar for ikke å bidra til å gjøre det enklere å få tilgang til personinformasjon som kan brukes av en identitetstyv.

Sikkerhet utenfor virksomheten

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikkerhet utenfor virksomheten (124839)

For IKT-medarbeidere skaper hjemmedatamaskiner, bærbare datamaskiner, nettbrett og smarttelefoner ekstra utfordringer.

Mange av de sikkerhetstiltakene som du normalt har full kontroll over, er overlatt til brukeren når datautstyret befinner seg på et hjemmekontor eller på reise.

Virksomheten bør derfor ha egne retningslinjer for bruk av datamaskiner utenfor kontoret. Spesielt gjelder dette bærbare maskiner som regelmessig flyttes mellom arbeidsplass og hjem, eller tas med på reiser.

Bedriften bør ha klare regler for hvordan jobbmaskiner skal håndteres på reise. Fotograf: Corbis

Reglene bør si noe om:

- **hvem som har lov til å bruke maskinen** – jobbmaskinen skal ikke være familie-pc
- **hva det er lov til å bruke maskinen til**
- **hva det er lov til å installere på maskinen**
- **hvilke data som ikke skal være lagret på maskinen** – for eksempel konfidensielle dokumenter, budsjetter, personopplysninger og så videre
- **hvordan maskinen skal sikres når den forlates** – for eksempel passordbeskyttelse, pc-lås eller annet

Selv om sikkerhet er viktig, må ikke reglene være så omfattende eller detaljerte at brukeren ikke klarer å huske dem, eller ikke orker å sette seg inn i dem.

Sammen med reglene bør det også være informasjon om hva brukerne bør være oppmerksomme på når de tar en maskin med på reise. Denne informasjonen bør si noe om usikrede nettverk, skuldertitting og faren for tyveri:

Usikrede nettverk

Hoteller, flyplasser, spisesteder og andre offentlige steder har ofte åpne trådløse nettverk. Slike nettverk kan ha dårlig sikkerhet som gjør at andre kan «avlytte» datatrafikken som sendes over nettet. I tillegg er maskinen mer utsatt for angrep.

Skuldertitting

På offentlige steder er det lett for andre å kikke over skulderen din mens du skriver på datamaskinen. Tenk derfor på hvordan du plasserer deg, og hva du bruker maskinen til på utsatte steder.

Faren for tyveri

Datautstyr og smarttelefoner er fristende bytte for tyver, og det hender også at datamaskiner blir gjenglemt i resepsjoner, avgangshaller eller på offentlige transportmidler. Selv om maskinen som regel er enkel å erstatte, kan informasjonen som ligger lagret på den, være uerstattelig.

- **Lenke**: IKT utenfor kontoret
- **Lenke**: IKT på reise i utlandet
- **Artikkel:** Drosjesjåfør stakk av med PC
- **Artikkel:** Topp-hemmelig PC forsvunnet

- **Artikkel:** Forfatter frastjålet manus til siste krimroman

Mange av de sikkerhetstiltakene som du normalt har full kontroll over, er overlatt til brukeren når datautstyret befinner seg på et hjemmekontor eller på reise.

Data i skyen

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Data i skyen (124845)

I tillegg til at datautstyr tas med utenfor bedriften, blir data stadig oftere også lagret på servere som virksomheten ikke har full kontroll over i det som kalles for «nettskyen».

Selv om slike tjenester kan være både rimelige og praktiske, er de ikke uproblematiske. Sikkerheten i de fleste tjenestene kan være god, men det vil alltid kunne skje feil som gjør at data kan gå tapt eller kommer på avveier.

I 2011 førte for eksempel en feil i en oppdatering til at det bare var nødvendig å skrive inn brukernavn for å få tilgang til kontoer hos den populære nettskytjenesten Dropbox. Siden Dropbox bruker eierens e-postadresse som brukernavn, var det i prinspippet fritt fram for alle. Feilen ble raskt oppdaget og rettet, men det viser at denne typen tjenester kan være sårbare.

Nettsky-tjenester (cloud computing).
Fotograf: C.J. Burton

Nettbasert lagring kan i mange tilfeller likevel være en god løsning, for eksempel når det er behov for å dele data med noen utenfor virksomheten. Denne typen lagring bør imidlertid ikke brukes til konfidensiell informasjon eller informasjon som kan misbrukes av andre hvis den kommer på avveie.

Som IKT-servicemedarbeider er det tre ting du bør være spesielt oppmerksom på:

1. Brukere tar ofte i bruk nettbaserte lagringstjenester uten å gi beskjed til IKT-avdelingen først. Videre registreres gjerne kontoen på brukeren privat, selv om den i hovedsak skal brukes i jobbsammenheng. Dette kan skape problemer når ansatte slutter i virksomheten.
2. Brukere velger ofte tjenester og tar dem i bruk uten å vurdere eventuell sikkerhetsrisiko.
3. Brukere vet ofte ikke hvordan de skal sette sikkerhetsinnstillinger for tjenesten riktig. Mange av de nettbaserte lagringstjenestene har mulighet for deling og publisering av data. Hvis brukerne ikke har tilstrekkelig kunnskap om slike funksjoner, risikerer de i verste fall å gjøre informasjon åpent tilgjengelig og søkbar på Internett uten å være klar over det.

Et annet problem med nettskylagring er at data som legges der, ikke kommer med i den vanlige sikkerhetskopieringen som virksomheten gjør av sine servere. Hvis ikke tjenesten inkluderer sikkerhetskopiering, eller brukeren selv sørger for å ta kopi, risikerer man at data går tapt hvis noen ved et uhell sletter eller endrer filer. Det har også forekommet at tjenesteleverandører har slettet brukeres data ved en feiltakelse.

De fleste problemene kan imidlertid unngås hvis virksomheten legger til rette for at de ansatte kan bruke nettbasert lagring på en trygg måte.

1. Velg en seriøs og profesjonell leverandør som tar sikkerhet på alvor, og som har løsninger for sikkerhetskopiering.
2. Opprett kontoer for brukerne som er registrert på virksomheten og ikke brukerne privat.
3. Gi brukerne opplæring i hvordan de skal bruke lagringstjenesten på en sikker måte.

- **Lenke:** Lagring i nettsky
- **Lenke:** Dette risikerer du ved å lagre filer i nettskyen

Brukere vet ofte ikke hvordan de skal sette sikkerhetsinnstillinger i nettbaserte lagringstjenester.

Anmelde sikkerhetsbrudd

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Anmelde sikkerhetsbrudd (124848)

Alvorlig datakriminalitet og sikkerhetsbrudd som datainnbrudd, informasjonstyveri, identitetstyveri, databedrageri og lignende bør anmeldes til politiet.

Norsk senter for informasjonssikring (NorSIS) har laget noen retningslinjer for hvordan en slik anmeldelse bør utformes og hva den bør inneholde. En anmeldelse bør inneholde:

1. navn, adresse og telefonnummer til den som anmelder saken
2. en beskrivelse av hva slags lovbrudd anmeldelsen gjelder, og en oversikt over fakta i saken
3. eventuell dokumentasjon som viser hva som har skjedd, og som kan være bevis i saken. Hvis det finnes vitner, bør kontaktinformasjon til disse være med.
4. eventuelle mistenkte. Hvis det er konkret mistanke til bestemte personer, bør disse oppgis med navn, adresse og/eller annen identifikasjon.
5. hvilke straffebestemmelser du mener er brutt
6. hva som er gjort før anmeldelsen når det gjelder mistenkte personer og sikring av bevis
7. om du mener lovbruddet gir grunnlag for erstatningsansvar, og størrelsen på erstatningskravet. Det er viktig å opplyse om at du ønsker at politiet skal ta erstatningskravet med i en eventuell straffesak.

Hacking kan være et alvorlig problem for enkelte bedrifter.

Hvis lovbruddet gjelder den virksomheten du jobber for, kan du ikke på egen hånd levere en anmeldelse. Det er egne regler i ulike lover for hvem som kan be om at noen skal tiltales og eventuelt straffes. I utgangspunktet er det virksomhetens styre som skal ta beslutning om anmeldelse, men dette er ofte delegert til daglig leder eller andre i virksomhetens ledelse. Det samme gjelder for krav om erstatning.

Lenke: NorSIS eksempel på anmeldelse

Alvorlig datakriminalitet bør anmeldes til politiet.

Sikkerhetsorganisasjoner

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Sikkerhetsorganisasjoner (124859)

Det finnes flere bransjeorganisasjoner og offentlige myndigheter som arbeider med IT-sikkerhet.

NSM – Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er et direktorat underlagt Forsvarsdepartementet. Deres hovedoppgave er å koordinere forebyggende sikkerhetstiltak og kontrollere sikkerheten i alle virksomheter som omfattes av sikkerhetsloven. Det gjelder blant annet stat og kommune, samt private virksomheter som er leverandører av sikkerhetsgraderte varer eller tjenester til det offentlige.

Dette omfatter langt mer enn IT-sikkerhet, men NSM har i stor grad oppmerksomheten rettet mot internettsikkerhet – blant annet gjennom NorCERT (Norwegian Computer Emergency Response Team) – Norges nasjonale senter for håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.

Bygget der Nasjonal sikkerhetsmyndighet (NSM) holder til på Kolsås base i Bærum.
Fotograf: Erlend Aas

SERTIT – sertifisering av IT-sikkerhet

I 2002 opprettet myndighetene en egen frivillig sertifiseringsordning for IT-sikkerhet i produkter og systemer. Ordningen administreres av SERTIT (Sertifiseringsmyndigheten for IT-sikkerhet) som er en del av Nasjonal sikkerhetsmyndighet.

SERTIT utformer nasjonale regler og rammeverk for IT-sertifisering, utnevner og følger opp virksomheter som skal evaluere sikkerhet, samt utsteder internasjonalt gyldige sertifikater og sertifiseringsrapporter.

Hensikten er å gi myndigheter og industri mulighet for å få en nøytral vurdering av IT-sikkerheten. Det skal igjen bidra til å styrke tilliten til og bedre sikkerhetsnivået i IT-produkter og systemer.

Andre viktige mål med ordningen er

- å styrke IT-sikkerheten i offentlig sektor
- å skape tillit til e-handelsløsninger og annen kommunikasjon nasjonalt og internasjonalt
- å bidra til å gjøre norsk IT-industri mer konkurransedyktig overfor utlandet
- å gjøre det enklere for innkjøper ved å styrke tilliten til at forhåndsdefinerte sikkerhetskrav er tilfredsstilt

NorSIS – Norsk senter for informasjonssikring

NorSIS ble opprettet som et prøveprosjekt av Regjeringen i 2002 og etablert som et permanent senter i 2006. NorSIS jobber for at informasjonssikkerhet i samfunnet skal bli en naturlig del av hverdagen gjennom å:

- bevisstgjøre om trusler og sårbarheter
- opplyse om konkrete tiltak gjennom nyheter, råd og veiledninger
- påvirke til gode holdninger innen informasjonssikkerhet

Målgruppa er norske virksomheter i privat og offentlig sektor.

Seniorrådgiverne Hans Marius Tessem (til høyre) og Vidar Sandland ved NorSIS på Gjøvik. Fotograf: Geir Olsen

ISF – Norsk Informasjonssikkerhetsforum

I S F er en ideell organisasjon som arbeider med informasjonssikkerhet for sine medlemmer. Målet er å samarbeide i prosjekter for å belyse og avklare trusler og sårbarheter for den enkelte organisasjonen. Både private og offentlige virksomheter kan bli medlemmer.

ITAKT – Internett- og telekombransjens antikriminalitetstiltak

ITAKT ble opprettet i 1999 og er en bransjeforening for å bekjempe svindel og misbruk av tjenestene og infrastrukturen til norske internett- og teleoperatører. Organisasjonens 15 medlemsbedrifter inkluderer alle de største mobiltelefonoperatørene og internettilbyderne i Norge.

- **Lenke:** NSM
- **Lenke:** Sikkerhetsbloggen – Blogg fra Nasjonal sikkerhetsmyndighet
- **Lenke:** NorCERT
- **Artikkel:** Toppledere utsatt for spionangrep
- **Lenke**: SERTIT
- **Lenke:** NorSIS
- **Lenke:** ISF
- **Lenke:** ITAKT

Oppgaver

Krypteringsaktivitet

Forfatter: Tron Bårdgård
Krypteringsaktivitet (131795)

Denne oppgaven lar elevene få prøve seg på kryptering av data på en grunnleggende og enkel måte. Den utfordrer elevene til å lage, tyde og knekke enkle koder/krypteringer ved bruk av forskjellige metoder.

Start med å dele klassen inn i for eksempel fem grupper. Hver gruppe skal kryptere en selvvalgt tekst, krypteringen gjøres med en selvlaget kodenøkkel. Hver gruppe har så en vennegruppe. Denne vennegruppa skal få deres krypterte kode og nøkkel. Hver gruppe har også en fiendegruppe som skal prøve å knuse koden, men bare ved å bruke den krypterte koden.

Gruppe * har	Vennegruppe	Fiendegruppe
1	2	3
2	3	4
3	4	5
4	5	1
5	1	2

Leken går i to faser. Først skal alle gruppene sette seg ned og lage sin kodete tekst. Dette gjør de på de tre arkene som ligger ved. Legg merke til at arkene til læreren, fiendegruppa og vennegruppa inneholder forskjellig informasjon (alle skal ha den samme kodete teksten).

Når alle gruppene er ferdige med å lage kodene, leverer de sine tre ark til læreren, som ser over at alt er rett.

- Læreren tar selv det fullstendige arket (med både råtekst, kryptert tekst og kodenøkkel).
- Læreren gir gruppas vennegruppe arket med koden og kodenøkkel.
- Læreren gir fiendegruppa arket som bare har koden.

Når alle gruppene har fått koden og nøkkelen fra vennegruppa, og koden fra fiendegruppa, skal de gå i gang med å prøve å løse kodene.

Når gruppene er ferdige, samles alle elevene, og man går gjennom hver enkelt gruppe og ser om de har klart å løse begge kodene.

Om ønskelig så kan man gi poeng under oppsummeringen. Hver gruppe kan eksempelvis få

- 2 poeng for å ha løst sin vennegruppes kode
- 2 poeng for å ha løst sin fiendegruppes kode
- 2 poeng for at deres kode ble løst av vennegruppa
- 2 poeng hvis deres egen kode ikke ble knust av fiendegruppa)

Følgende dokumenter kan skrives ut, og brukes i forbindelse med denne aktiviteten:

Krypteringsaktivitet - Til lærer / fil
http://ndla.no/nb/node/131791

Krypteringsaktivitet - Til vennegruppe / fil
http://ndla.no/nb/node/131793

Krypteringsaktivitet - Til fiendegruppe / fil
http://ndla.no/nb/node/131789

Fagbegreper

Fagspråk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Fagspråk (119607)

For å kunne kommunisere med kollegaer, leverandører og andre i databransjen må du kunne faguttrykkene.

Vi skiller mellom **fagspråk** og **dagligspråk**. Dagligspråk, også kalt allmennspråk, er slik vi snakker når vi bruker vanlige ord som de aller fleste forstår.

Men i dagligspråket kan det samme ordet ha flere betydninger, eller betydningen kan være avhengig av sammenhengen eller situasjonen. Det gjør at dagligspråket noen ganger blir litt for upresist. De fleste bransjer har derfor sitt eget fagspråk i form av faguttrykk, betegnelser og begreper som har en mer presis og avgrenset betydning enn dagligspråket. Vi kaller dette for **fagterminologi**.

Fagterminologi er ord og uttrykk som brukes innenfor et avgrenset fagområde. Hensikten er å gjøre utveksling av fagkunnskap og kommunikasjon mellom dem som arbeider innenfor fagområdet, lettere og mer entydig. Alle bransjer og yrker har en egen fagterminologi, men det varierer hvor omfattende fagterminologien er.

Som IKT-servicemedarbeider forventes det at du forstår fagterminologien i databransjen og kan bruke ord og uttrykk riktig.

Det er viktig å kunne fagterminologien for å kunne kommunisere med kollegaer og kunder.

Lenker:

- TechTarget WhatIs.com – engelskspråklig IT-leksikon
- Webopedia – engelskspråklig IT-leksikon
- Hardware.no dataordbok – tekniske uttrykk og forkortelser

Det er flere grunner til at det er viktig å kjenne fagterminologien:

- for å forstå hva som blir sagt når du snakker med kollegaer, leverandører eller andre i databransjen
- for å forstå hva som står i håndbøker og hjelpfunksjoner
- for å kunne dokumentere systemer på en riktig måte
- for å kjenne tilhørighet og yrkesstolthet

Det tar tid å lære alle faguttrykkene, og du vil oppleve at det stadig dukker opp nye begreper som du ikke har hørt før. Ikke fall for fristelsen til å bløffe og late som du forstår et uttrykk du ikke har hørt før. Spør eller slå opp ord du ikke er sikker på hva betyr.

Du finner forklaring på de aller fleste datauttrykk i IT-leksikon på nettet som WhatIs.com og Webopedia. I tillegg er den engelske utgaven av Wikipedia et godt oppslagsverk for IKT-begreper og teknologier.

Mange IKT-servicemedarbeidere jobber med IKT i virksomheter som er i en helt annen bransje, og som har sin egen fagterminologi. Det skaper ekstra utfordringer, og du må være forberedt på at du da også må lære fagterminologien for virksomhetens bransje for å kunne gjøre en god jobb.

> Som IKT-servicemedarbeider forventes det at du forstår fagterminologien i databransjen og kan bruke ord og uttrykk riktig.

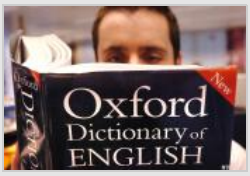
Norsk eller engelsk?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Norsk eller engelsk? (119629)

Databransjen bruker svært mange engelske faguttrykk og forkortelser, og mange av disse har ikke noen entydig norsk oversettelse.

Håndbøker og hjelpfunksjoner for serversystemer og nettverksutstyr finnes vanligvis bare på engelsk, og på de fleste fora og hjelperessurser på Internett er språket engelsk. Så du må være forberedt på å lese og forstå mye engelsk når du driver for eksempel feilsøking.

Mange engelske datauttrykk har ikke noen direkte eller entydig norsk oversettelse, men der det finnes gode norske ord, bør du bruke dem – spesielt når du kommuniserer med brukere. Bruk for eksempel «skriver» istedenfor «printer», «minnepinne» istedenfor «USB-stick» og «mappe» istedenfor «folder».



Lenke:

- Språkrådet fornorsker dataspråket – artikkel og innslag fra NRK

Men alt bør ikke oversettes for enhver pris. I mange tilfeller er det ikke noen etablert noen norsk oversettelse, og å forsøke å oversette på egen hånd kan lett føre til misforståelser.

Det er heller ikke alle oversettelser som har festet seg i språket. For eksempel forstår de fleste hva du mener hvis du sier «webmaster» eller «chat». Ikke alle er like fortrolige med de norske oversettelsene «vevadministrator» og «prateprogram».

En annen ting er at de norske bokstavene *æ, ø og å* av og til skaper problemer for noen programmer. Men dette er selvsagt ikke et argument for å bruke engelske ord og uttrykk når du snakker.

Når det finnes gode norske ord, bør du bruke dem.

Når skal du ikke bruke fagspråk?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Når skal du ikke bruke fagspråk? (119630)

Like viktig som å bruke de riktige uttrykkene når du kommuniserer med andre i bransjen, er det å bruke dagligspråk når du kommuniserer med brukere.

Å bruke faguttrykk faller ofte naturlig, og vi vil jo gjerne forklare så nøyaktig som mulig, men vi risikerer å forvirre mer enn vi opplyser hvis vi bruker fagterminologi som andre ikke forstår. Du kan selv tenke deg hvordan du ville følt det hvis du gikk til en lege og han brukte medisinsk fagterminologi for å forklare hva som var galt, og hva du måtte gjøre.

Når du bruker fagterminologi i samtaler med kollegaer og andre i samme bransjen, bidrar det til å skape tilhørighet. Men når du gjør det i samtale med brukere og andre som ikke er like opptatt av IKT, kan det tvert imot skape distanse mellom deg og brukeren.

Noen tror også at det å bruke fagterminologi får dem til å virke smartere, eller de bruker mange faguttrykk for å vise hvor mye de kan. Det fører i beste fall til at de blir oppfattet som dårlige til å kommunisere, og i verste fall til at de ses på som arrogante og nedlatende.

Unngå å benytte fagspråk som hersketeknikk. Brukeren forstår ikke hva du sier, og selv vil du fremstå som arrogant og lite samarbeidsvillig.

Lenker:

- IKT og språk – fra Språkrådet
- Dataspråk forvirrer ansatte – artikkel fra Computerworld

Enda verre er det hvis fagspråk blir brukt eller sett på som en måte å vise makt og overlegenhet på. Det kan skje når IKT-medarbeidere bevisst bruker sitt fagspråk for å demonstrere at de kan mer enn brukerne, vel vitende om at brukerne ikke forstår hva de sier. Fagspråk blir da en form for hersketeknikk. Derfor må du tilpasse språket og bruke mer dagligspråk og mindre fagspråk – avhengig av hvem du snakker med.

Det er lett å glemme at ord og begreper som det er naturlig å benytte i IKT-sammenheng, ikke alltid blir forstått av dem som ikke jobber med IKT til daglig. Selv betydningen av vanlige begreper som er opplagte for deg, kan være ganske uklare for brukeren.

Det er for eksempel ikke uvanlig å tro at harddisken er det samme som hele datamaskinen. Så hvis du sier at harddisken må skiftes, tror brukeren kanskje at han skal få en ny datamaskin. Om du må skifte minne, kan du kanskje si følgende til en fagperson: «Vi må kjøpe inn 4 GB ekstra RAM til en laptop av typen HP ProBook 6570b». Til brukeren velger du kanskje heller å si: «For å gjøre PC-en raskere må vi oppgradere minnet i din bærbare PC.»

Det er heller ikke noen skarp overgang mellom dagligspråk og fagspråk, og mange ord som starter som faguttrykk, blir gradvis innarbeidet i dagligspråket etter hvert som flere forstår dem og tar dem i bruk. Ord som ikon, dobbelklikke og app (applikasjon) var en gang faguttrykk, men i dag forstår og bruker de fleste dem.

Tilpass språket og bruk mer dagligspråk og mindre fagspråk når du snakker med brukere.

Virksomhetsstøtte

Kostnads- og nytteverdi

Dokumentere IKT-bruk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Dokumentere IKT-bruk (109281)

En virksomhet har behov for å følge med på og dokumentere IKT-bruken.

Det er flere grunner til å følge med på og dokumentere IKT-bruken i en virksomhet. Blant annet vil vi

- sørge for at maskinressurser brukes på best mulig måte og der de gjør mest nytte for seg
- holde oversikt over hvilke programvarelisenser virksomheten trenger og skal betale for
- kunne forutse og planlegge det behovet vi får for utstyr og kapasitet framover

Kapasitetsbehov

Brukere har vanligvis ulike arbeidsoppgaver og ulikt behov for datautstyr. Ved å kartlegge de enkelte brukeres behov kan vi sørge for at maskiner, skjermer og skrivere fordeles slik at en bruker med et stort behov for maskinressurser, ikke blir sittende med en for dårlig maskin, mens en bruker med et lite behov for maskinressurser, sitter med en kraftig maskin uten å bruke ressursene.

Lisenser

En annen viktig grunn til å dokumentere IKT-bruken er for å ha oversikt over hvilke programvarelisenser virksomheten trenger og skal betale for.

Virksomheten ønsker ikke å betale for flere lisenser enn den trenger. Samtidig må vi være sikre på at vi ikke bruker programmer uten å betale for dem – det er i praksis det samme som å bruke piratkopiert programvare.

Programvarelisenser kan være knyttet til

- antall brukere
- antall samtidige brukere
- antall maskiner programmet er installert på

For en lisens som er knyttet til **antall brukere**, betaler vi for hver person som bruker programmet, men hver person kan godt ha programmet installert på flere maskiner.

For en lisens som er knyttet til **antallet samtidige brukere**, betaler vi bare for en viss mengde brukerer som kan bruke programmet samtidig. Slike lisenser benyttes blant annet for mange serverbaserte eller internettbaserte applikasjoner. Hvis vi for eksempel har lisens for 20 samtidige brukere av et program, og alle lisensene er i bruk, vil en ny bruker ikke få tilgang til programmet før en annen logger seg ut.

For en lisens som er knyttet til **antall maskiner** programmet er installert på, betaler vi for antallet installasjoner uavhengig av hvor mange som bruker programmet. Du kan også komme over programmer som bruker en kombinasjon av ulike lisenstyper.

> Vi ønsker ikke å betale for flere lisenser enn vi trenger, men vi må også være sikre på at vi ikke bruker programmer uten å betale for dem.

Kapasitetsovervåking

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kapasitetsovervåking (109283)

En annen grunn til å dokumentere IKT-bruken er for å kunne forutse framtidige behov for oppgraderinger. Da får vi gjort de nødvendige oppgraderingene før det oppstår en flaskehals eller et problem. Vi kaller dette for kapasitetsovervåking.

Kapasitetsovervåking er vesentlig for budsjettering av framtidige IKT-investeringer. Ledelsen i bedriften forlanger normalt å få et budsjett for nødvendige investeringer i forbindelse med den årlige budsjettbehandlingen. Du bør derfor være i stand til å kunne forutse nødvendige oppgraderinger opptil ett år i forveien. Uforutsette budsjettoverskridelser blir sjelden godt mottatt i noen virksomhet.
Kapasitetsovervåking innebærer at vi har en rutine for å overvåke bruken av og belastningen på de ressursene som kan være en begrensning eller bli en flaskehals. Det som er vanlig å holde et øye med, er:

- **lagringsplass:** harddiskplass på servere og arbeidsstasjoner, samt kapasitet på media for sikkerhetskopiering
- **nettverkskapasitet:** tilstrekkelig hastighet på internt nettverk og internettilgang
- **serverkapasitet:** serverparkens mulighet til å betjene det forventede antallet brukere og forespørsler – det siste er særlig aktuelt i forbindelse med applikasjonsservere
- **skriverressurser:** tilstrekkelig kapasitet til å håndtere bedriftens utskriftsvolum

De fleste operativsystemer er utstyrt med verktøy for å måle ressursbelastningen. I tillegg finnes det en rekke systemer som er utviklet spesielt for ressursovervåking. Selve informasjonsinnsamlingen er vanligvis automatisert slik at belastningen på ulike ressurser automatisk registreres på fastsatte tidspunkter.

Kapasitetsplanlegging er nærmere beskrevet i kompetansemål 5, *Yte service gjennom driftsstøtte og kommunikasjon med leverandører og fagpersonell på norsk og engelsk,* i faget Bruker og driftsstøtte.

Det er viktig å overvåke bedriftens serverkapasitet slik at du tidlig kan varsle om eventuelle behov for oppgraderinger.

Kapasitetsovervaking er vesentlig for budsjettering av framtidige IKT-investeringer.

Vurdere kostnader og nytteverdi 1

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vurdere kostnader og nytteverdi 1 (109284)

Selv om det vanligvis ikke er IKT-servicemedarbeideren som tar avgjørelser om virksomhetens IKT-strategi eller større investeringer, er det ikke alltid ledelsen har den nødvendige IKT-fagkunnskapen til å kunne forutsi konsekvensene av for eksempel å oppgradere til en ny teknologi. IKT-medarbeidere blir derfor ofte trukket inn i slikt arbeid.

Samtidig er det viktig å være oppmerksom på at teknologikunnskap ikke alltid er den viktigste bakgrunnen for å kunne ta riktige avgjørelser om IKT-investeringer.

Mange virksomheter har gjort kostbare feilinvesteringer fordi virksomhetens IKT-medarbeidere har argumentert for løsninger basert på sine egne ønsker og meninger ut fra rene tekniske forutsetninger, uten å ta hensyn til hva virksomheten egentlig har behov for.

La oss se på ett enkelt eksempel:

Tenk deg at du arbeider i en virksomhet som bruker Microsoft Office til vanlige kontoroppgaver som tekstbehandling, regneark og presentasjoner. Microsoft kommer med en ny versjon av Office-pakken, og spørsmålet er om virksomheten bør oppgradere.

Hvis du spør Microsoft, vil svaret garantert være ja, og som IKT-servicemedarbeider er du antakelig tilbøyelig til å være enig. En ny programversjon har nye funksjoner og muligheter, og det er jo viktig å henge med i utviklingen. Kanskje har du også brukt den nye versjonen på din egen pc i lang tid allerede.

Men å oppgradere en programpakke på én enkelt pc eller en hjemme-pc er imidlertid noe helt annet enn å gjøre den samme oppgraderingen for et stort antall brukere i en virksomhet. Selv små endringer kan medføre store kostnader i tillegg til prisen på selve programpakken (lisenskostnadene). Eksempel på dette er:

- **tida som går med til arbeidet med oppgraderingen:** Dette er betalt arbeidstid, og ofte må oppgraderinger av denne typen gjøres utenom vanlig arbeidstid for å unngå at brukerne får avbrutt arbeidsdagen sin. Du må også ta med den tida som går med til testing før selve oppgraderingen gjennomføres, med i beregningen.
- **opplæring av brukerne** for at de skal kunne nyttiggjøre seg nye funksjoner
- **tida som går med til ekstra brukerstøtte** fordi brukerne ikke kjenner nye funksjoner, eller fordi kjente funksjoner ikke fungerer på samme måte som tidligere
- **eventuell ekstra tid som brukerne trenger for å orientere seg** i programmet og gjøre seg kjent med funksjoner som er endret eller er nye
- **eventuell tid som går med til feilsøking og retting av feil** som følge av programendringen. Dette kan for eksempel være problemer som oppstår ved utveksling av data med andre systemer, makroer som ikke fungerer slik de skal lenger, konvertering av eldre data og lignende
- **eventuelt maskinutstyr som må oppgraderes** som følge av økte systemkrav for den nye programpakken

Det kan være fristende alltid å oppgradere til nyeste programvare eller operativsystem, men er det lønnsomt? Her presenterer Windows-president Steven Sinofsky Windows 8 operativsystem i oktober 2012.
Fotograf: Justin Lane

Selv om ikke alle disse kostnadene nødvendigvis er relevante for en Office-oppgradering, er de likevel representative for en typisk programoppgradering.

De totale kostnadene for oppgraderingen må så veies opp mot den nytteverdien oppgraderingen har for virksomheten.

- Har den nye programpakken funksjoner som virksomheten trenger eller savner i dag?
- Vil oppgraderingen gjøre arbeidet mer effektivt?
- Vil oppgraderingen medføre reduserte kostnader i form av mindre brukerstøtte og service i framtida?
- Oppnår virksomheten noen form for konkurransefordel som følge av oppgraderingen?
- Hvor lang tid vil det ta før effektiviseringen eller konkurransefordelen vil ha tjent inn kostnadene?
- Er det noen problemer med den versjonen virksomheten har i dag, som løses ved oppgraderingen?

Hvis vi nå antar at virksomheten bare benytter Office-pakken til litt brev- og dokumentskriving i Word, noen standard regnearkmodeller og noen PowerPoint-presentasjoner, vil det som regel være vanskelig å forsvare de kostnadene en oppgradering medfører. Det er altså ofte gode grunner til at mange virksomheter velger å beholde gamle programversjoner så lenge som mulig.

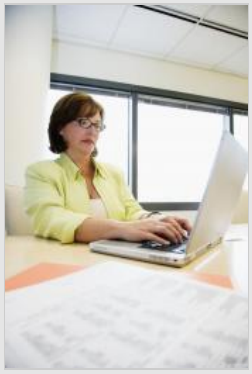
Eksempelet er enkelt, men likevel svært typisk. Det er heller ikke urealistisk med tanke på de vurderingene du av og til blir stilt overfor i jobben som IKT-servicemedarbeider.

Andre viktige vurderinger

Vi valgte eksemplet med en programoppgradering over fordi den er enkel å forholde seg til, men det finnes en rekke andre og ofte langt mer alvorlige feilvurderinger vi kan gjøre. For eksempel:

- innføre ny teknologi som ikke er tilstrekkelig testet ut på områder som er kritiske for virksomheten
- undervurdere kostnadene ved å innføre nye systemer
- undervurdere konsekvensene for andre deler av virksomheten ved innføring av nye systemer, eller endring av eksisterende systemer
- overvurdere nytteverdien av nye systemer eller endringer i eksisterende systemer
- vente for lenge med å innføre nye systemer

Husk å ta med i beregningen hvor mye tid og ressurser det vil gå med til å implementere en ny programvare.
Fotograf: C. Devan



Det er viktig å vurdere hvilke faktiske behov bedriften har før man gjennomfører en større oppgradering.
Fotograf: Corbis

Kostnadene ved en IKT-investering må vurderes opp mot de fordelene investeringen gir.

Vurdere kostnader og nytteverdi 2

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vurdere kostnader og nytteverdi 2 (109285)

Et annet enkelt eksempel på vurdering av kostnader og nytteverdi er valg av kontorstøttesystem.

Så å si alle virksomheter har bruk for standard kontorprogramvare for tekstbehandling, regneark og presentasjon. Det finnes flere muligheter, men vi kan tenke oss at en virksomhet har begrenset alternativene til Microsoft Office, OpenOffice.org og Google Dokumenter.

De dekker alle de samme grunnleggende programbehovene, men der er også forskjeller som vi må ta hensyn til.

Microsoft Office:

- innarbeidet standard som er godt kjent
- pris frå 2000 til 5000 kroner per maskin avhengig av lisenstype
- kan installeres på server eller på frittstående maskiner
- integrert med Outlook
- stort utvalg av dokumentasjon, lærebøker og kurs er tilgjengelig på norsk
- brukerstøtte fra Microsoft eller forhandler

OpenOffice.org

- ikke fullt så kjent
- gratis
- kan installeres på frittstående maskiner, men har begrenset nettverksstøtte
- kan lese og skrive Microsoft Office-dokumenter
- begrenset dokumentasjon på norsk
- brukerstøtte fra «community»

Google Dokumenter

- ganske godt kjent
- gratis
- ingen installasjon, men krever Internett
- mulighet for tilgang til dokumenter fra alle internettilkoblede maskiner
- mulighet for samskriving og samtidig redigering
- mulighet for å dele dokumenter enkelt med andre
- begrenset funksjonalitet sammenlignet med Microsoft Office og OpenOffice
- kan importere enkle dokumenter fra Microsoft Office og OpenOffice
- lite dokumentasjon på norsk
- begrenset brukerstøtte

Når vi kjenner produktenes egenskaper, kan vi vurdere dem opp mot behovene som virksomheten og brukerne har.

Hvis for eksempel pris er vesentlig, er det fristende å velge OpenOffice eller Google Dokumenter, siden disse er gratis. Men som du så i eksempelet med oppgradering av programvare, kan det være andre kostnader som du må ta hensyn til. Hvis brukeren allerede kan bruke Microsoft Office, kan valg av en annen pakke medføre store kostnader til blant annet opplæring og brukerstøtte.

Hvis det derimot er vesentlig at brukerne enkelt skal kunne dele dokumenter med personer utenfor virksomheten, er antakeligvis Google Dokumenter det beste valget – forutsatt at man ikke trenger de mer avanserte funksjonene som Microsoft Office og OpenOffice har.

Microsoft Office

Fotograf: Mike Blake

Google

Fotograf: Mark Lennihan

Målet er å finne den beste balansen mellom kostnader og nytteverdi.

Det lønner seg å gå systematisk til verks. Ved å sette opp en oversikt over hvilke krav og ønsker vi har til et produkt, og sammenligne dem med egenskapene til de produktene vi kan velge mellom, blir det lettere å vurdere nytteverdien og kostnadene for hvert enkelt produkt.

Som regel finner vi ikke ett enkelt produkt som både tilfredsstiller alle krav og ønsker, og som samtidig gir de laveste kostnadene. Målet er derfor å finne den beste balansen mellom kostnader og nytteverdi.

Økt kompleksitet gir økte kostnader

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Økt kompleksitet gir økte kostnader (109286)

Jo mer komplisert et IKT-system blir, jo høyere blir kostnadene ved å drifte det. Som IKT-servicemedarbeider må du derfor alltid vurdere om det du foretar deg, fører til økt kompleksitet i systemet.

La oss se på et enkelt eksempel. Anta at du må skifte et defekt nettverkskort i en pc. Et nytt nettverkskort av samme merke koster 400 kroner, men du finner et tilsvarende fra en annen produsent som bare koster 300 kroner, og velger dette i stedet. Du kan dermed gratulere deg selv med at du har spart virksomheten for en unødig utgift på 100 kroner. Men samtidig har du også økt kompleksiteten i nettverket, og det kan fort koste mye mer enn de 100 kronene du sparte.

Nettverkskort med antenne.
Fotograf: Espen Bratlie

Små endringer og utskiftninger kan fort øke kompleksiteten og gjøre det vanskeligere å løse problemer.
Fotograf: Corbis

Jo mer komplisert et IKT-system blir, jo høyere blir kostnadene ved å drifte det.

Siden du har fått et nytt nettverkskort fra en annen produsent i en av maskinene, trenger du antakelig også en egen driver til dette kortet. Nettverkskortprodusenter oppdaterer som regel sine drivere med jevne mellomrom for å rette feil eller forbedre funksjonalitet, ytelse eller kompatibilitet.

En IKT-avdeling vil gjerne legge opp en rutine for oppgraderinger av drivere tilsvarende det man gjør for serviceoppgraderinger av operativsystemer. Det vil si mest mulig automatisert og sentralt styrt.

Men du har fått en maskin som krever spesialbehandling fordi den ikke bruker den samme nettverkskortdriveren som de andre maskinene. Dermed er du i den situasjonen at du må kontrollere driveroppgraderinger fra to produsenter. Då må du enten lage et eget oppgraderingsoppsett for den maskinen som har det nye nettverkskortet, eller gjøre alle oppgraderinger av nettverkskortdriver manuelt på den maskinen.

Du kan også få problemer og ekstra arbeid hvis det dukker opp maskin- eller programvare som må konfigureres spesielt for det nettverkskortet det skal kommunisere med. Nok en gang vil denne maskinen kreve spesialbehandling. Et ukjent nettverkskort kan videre ha feil som er ukjente for deg, og som krever ekstra tid til feilsøking og løsing, mens problemer med de andre kortene etter hvert er godt kjente og kan løses raskt.

Selv om det i praksis som regel ikke vil medføre så store problemer å benytte et annet nettverkskort, illustrerer eksempelet over hvordan selv små endringer som øker kompleksiteten, kan få økonomiske konsekvenser som ikke alltid er like åpenbare. De fleste beslutninger av denne typen virker små og ubetydelige der og da, men over tid vil de sakte, men sikkert akkumuleres og etter hvert utgjøre en betydelig ekstra kostnad i form av merarbeid.

Et bevisst forhold til det å holde kompleksiteten på et så lavt nivå som mulig uten å ofre funksjonaliteten, er derfor et viktig bidrag til å holde kostnadene nede over tid.

Kravdefinisjon

Innledning til IKT-støtte i arbeidsprosesser

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innledning til IKT-støtte i arbeidsprosesser (123578)

Ingen virksomheter har datautstyr for utstyrets egen skyld. Datautstyr og datasystemer er verktøy som skal hjelpe virksomheten med å løse oppgaver og effektivisere arbeidsprosesser.

En arbeidsprosess er ganske enkelt en serie aktiviteter som gjøres for å produsere et bestemt resultat, for eksempel å ta imot bestillinger fra kunder og å sende ut varene.

I en virksomhet griper mange ulike arbeidsprosesser inn i hverandre, og hver prosess involverer ofte flere personer.

Når vi skal effektivisere en arbeidsprosess ved å bruke IKT, starter vi med å kartlegge selve arbeidsprosessen. Dette gjør vi ved å lage et prosessflytdiagram som viser de ulike trinnene i prosessen og forholdet mellom dem.

IKT-verktøy kan gjøre det mer effektivt å utføre arbeidsoppgavene i en bedrift.

Fotograf: Bjørn Rørslett

Når arbeidsprosessen er kartlagt, må vi identifisere de ulike rollene i prosessen. Med det menes hvilke personer som skal utføre og ha ansvaret for hvert enkelt trinn i prosessen. I tillegg er det gjerne også en prosesseier som har ansvaret for prosessen som helhet.

Som nytilsatt IKT-medarbeider er det viktig å få god oversikt over hva forskjellige personer i virksomheten jobber med. I starten kan det være lurt å lage en oversikt over hvilke oppgaver og ansvarsområder den enkelte ansatte har.

Når prosessen og rollene er avklart, kan vi begynne å identifisere behovet for IKT-støtte og vurdere hva slags IKT-løsninger (utstyr og programvare) som vil gi det beste resultatet for hver oppgave. I tillegg må vi også huske å vurdere behovet for opplæring og brukerstøtte.

Slike vurderinger må selvsagt gjøres sammen med de ansatte og ledelsen. Selv om det er IKT-medarbeiderne som har IT-kompetansen, kan de ikke sitte innelukket på et kontor og gjøre alle vurderinger og ta alle avgjørelser på egen hånd.

En arbeidsprosess er en serie aktiviteter som gjøres for å produsere et bestemt resultat.

Å lage et prosessflytdiagram

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Å lage et prosessflytdiagram (123582)

Et prosessflytdiagram er et diagram som viser stegene i en arbeidsprosess. Prosessflytdiagrammet gjør det enklere å se helheten i prosessen og sammenhengen mellom de ulike stegene og arbeidsoppgavene.

Prosessflytdiagrammer kalles også for arbeidsflytdiagrammer eller bare flytskjema.

Flytskjema bruker fastsatte symboler for å vise de ulike stegene i prosessen og forholdet mellom dem. Illustrasjonen under viser de mest brukte symbolene, men det finnes flere for mer spesialiserte oppgaver.

Flytskjema med symboler.

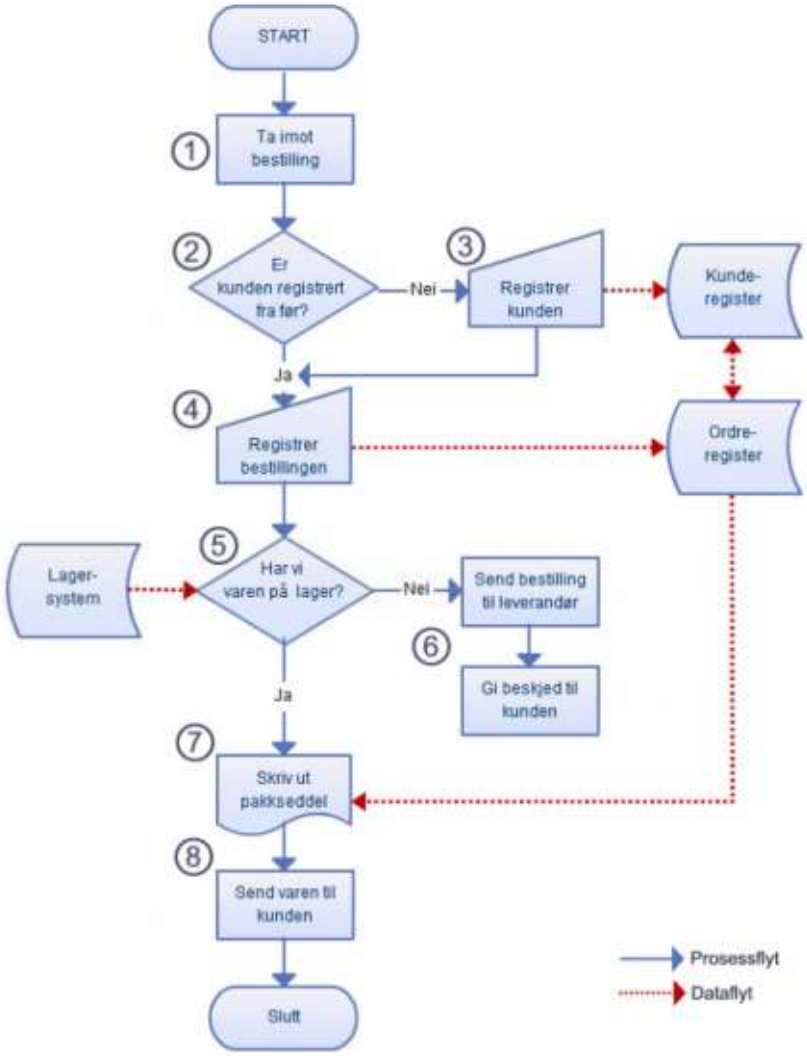
Opphavsmann: Arne Jansen

Et flytskjema kan godt tegnes for hånd, men det er som regel bedre å bruke et dataverktøy. Mange vanlige kontorstøtteprogrammer som tekstbehandling, regneark og presentasjonsprogram har innebygget flytskjemasymboler, og det finnes en rekke spesialprogrammer og nettbaserte verktøy.

Det lønner seg gjerne å lage en kladd før du begynner å tegne flytskjema i et program. En effektiv metode er å bruke Post-It-lapper på ei tusjtavle. Skriv alle oppgaver, registreringer, beslutninger og så videre på hver sin lapp, klistre lappene på tavla og tegn piler mellom dem. Etter hvert som du oppdager nye oppgaver, kan du lage nye lapper og flytte dem rundt på tavla inntil hele prosessen er kartlagt.

Eksempel på flytskjema

Eksempelet under viser et flytskjema for hvordan en virksomhet tar imot bestillinger fra kunder og sender ut varene.



Bestillinger fra kunder og ekspedering av ordre framstilt med et flytskjema.

Opphavsmann: Arne Jansen

1. Prosessen starter med at vi tar imot bestillingen fra kunden.
2. Før vi kan registrere bestillingen må vi finne ut om kunden er registrert. Dette markeres som en beslutning fordi svaret fører til to ulike handlinger.
3. Hvis kunden ikke er registrert fra før, må vi først registrere kunden i et kunderegister.
4. Når kunden er registrert, kan vi registrere bestillingen. Dette gjør vi i et ordreregister. Legg merke til pilen mellom kunderegisteret og ordreregisteret. Den markerer at disse systemene kommuniserer med hverandre.
5. Når bestillingen er registrert, må vi sjekke om varen er på lager. Informasjonen om dette finnes i et lagersystem.
6. Hvis varen ikke er på lager, må vi sende en bestilling til leverandøren og gi beskjed til kunden om når varen vil bli levert.
7. Når varen er på lager, skriver vi ut en pakkseddel fra ordreregisteret.
8. Til slutt sendes varen til kunden og prosessen avsluttes.

I dette flytskjema har vi forenklet en del. Det viser for eksempel ikke faktureringsrutiner, bestillingsrutiner eller hva som skjer når varer kommer fra leverandører og legges på lager. Men i mange tilfeller er en slik forenkling nødvendig for å unngå at diagrammet blir for komplisert. En arbeidsprosess består ofte av flere delprosesser eller har koblinger til andre prosesser.

Å forsøke å tegne alle prosesser inn i et kjempediagram kan lett bli uoversiktlig, og det lønner seg derfor å kartlegge og tegne hver prosess separat.

Lenke: Creately – nettbasert verktøy for å lage flytskjema og andre typer diagrammer.

Prosessflytdiagrammet gjør det enklere å se helheten i prosessen og sammenhengen mellom de ulike stegene og arbeidsoppgavene.

Identifisere roller i prosessen

Forfatter: Arne Jansen, NKI Forlaget
Identifisere roller i prosessen (123585)

Når prosessen er kartlagt, fortsetter vi med å identifisere hvilke roller som utfører de enkelte stegene i prosessen.

Selv om rollene i en arbeidsprosess fylles av personer, forsøker vi å unngå å bruke personnavn når vi skal dokumentere en prosess. I stedet bruker vi stillingsbetegnelser. Det gjør at vi ikke trenger å endre på rollene i prosessen hvis noen slutter og nye personer blir ansatt. Ofte vil den samme rollen også omfatte flere personer. En virksomhet kan for eksempel ha mange ordremottakere, kundebehandlere, lagermedarbeidere og så videre.

I eksempelet med prosessen for bestilling og utsendelse av varer kan vi tenke oss at de fire første oppgavene – å ta imot bestillingen og registrere kunden og bestillingen – gjøres av en ordremottaker.

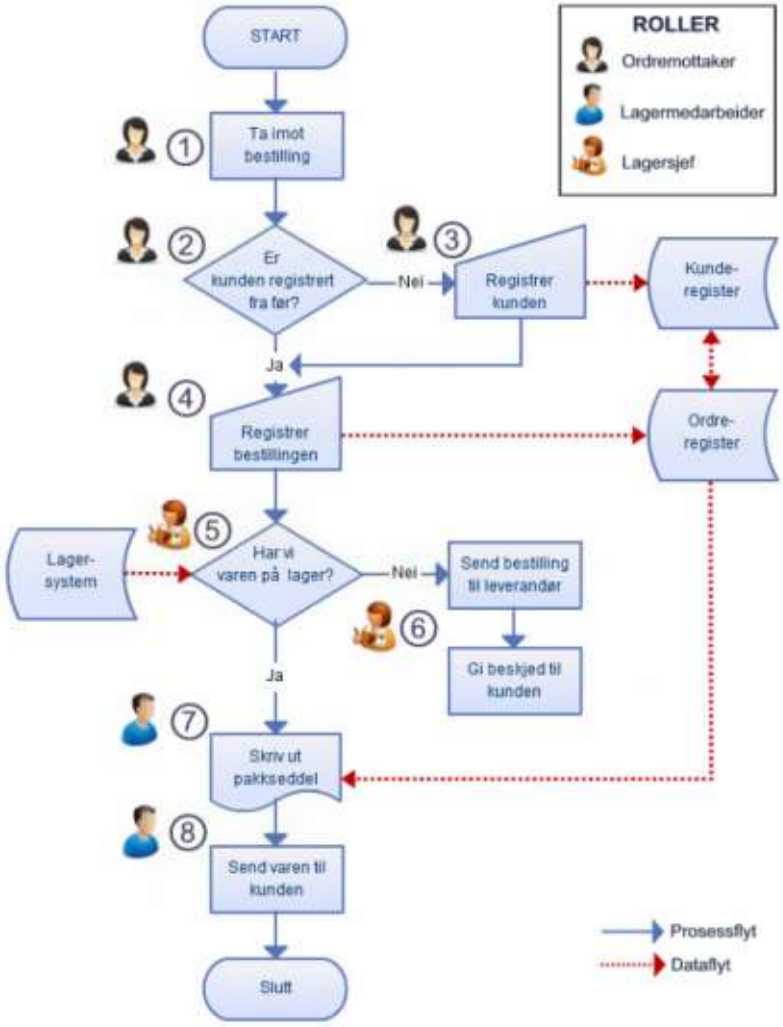
Oppgave 5 og 6: Lagersjefen sjekker om varen er på lager og sender eventuelt bestilling og informerer kunden.

Oppgave 7 og 8: En lagermedarbeider skriver ut pakkseddel og sender varen.

Vi får da tre roller i prosessen:

- ordremottaker (oppgave 1 til 4)
- lagersjef (oppgave 5 og 6)
- lagermedarbeider (oppgave 7 og 8)

Diagrammet under viser hvor rollene er plassert i prosessen.



Bestillinger fra kunder og ekspedering av ordre framstilt med et flytskjema og roller.

Opphavsmann: Arne Jansen

Selv om rollene i en arbeidsprosess fylles av personer, forsøker vi å unngå å bruke personnavn når vi skal dokumentere en prosess.

Vurdere behovet for IKT-støtte

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vurdere behovet for IKT-støtte (123588)

Når prosessen er kartlagt og rollene er identifisert, går vi over til å vurdere behovet for IKT-støtte.

Vi kan dele behovet for IKT-støtte i en arbeidsprosess inn i to kategorier:

1. systemer som inngår som en del av prosessen
2. systemer som den enkelte rolle trenger for å gjøre sine oppgaver i prosessen

Systemer som inngår som en del av prosessen, kalles for **prosesskritiske**. Det vil si at hele prosessen stopper opp hvis de ikke fungerer.

I eksemplet vi har brukt, er de prosesskritiske systemene allerede satt inn i form av kunderegister, ordreregister og lagersystem. Hvis for eksempel ordreregisteret ikke fungerer, eller serveren det kjører på, går ned, er det ikke lenger mulig å registrere ordrer, og prosessen stopper.

Prosesskritiske systemer er ofte del av en større vurdering. Et kunderegister er for eksempel ikke bare nødvendig for å registrere og effektuere bestillinger. Det vil også inngå i blant annet faktureringsrutiner og kan også være viktig i salgs- og markedsføringssammenheng.

Når vi skal vurdere behovet for IKT-støtte for prosesskritiske systemer, må vi derfor se på helheten og hvordan ulike prosesser griper inn i og overlapper hverandre.

En vurdering av et prosesskritisk system vil være mer omfattende enn det som kreves for den enkelte rolle. Vanlige spørsmål vil være:

- Hva slags programvare skal systemet baseres på?
- Er det behov for spesialtilpassing?
- Hvilke krav til driftssikkerhet og datasikkerhet må systemet tilfredsstille?
- Hva slags maskinutstyr krever systemet?
- Hvilke driftsrutiner må etableres for å drifte systemet?
- Hva er behovet for vedlikeholdsavtale, serviceavtale eller ekstern support?

Systemer som den enkelte rolle trenger for å gjøre sine oppgaver i prosessen, er vanligvis ikke prosesskritiske. Vurderingen av disse er derfor vanligvis enklere:

Vurder helheten når du skal anbefale IKT-støtte til arbeidsprosesser.
Fotograf: NTB scanpix

Behovet for ekstern support bør også vurderes når prosesskritiske system kartlegges.
Fotograf: Science Photo Library

- Hva slags utstyr trenger rollen?
- Hvilken programvare trenger rollen?
- Hvilke tilganger til prosesskritiske systemer trenger rollen?
- Hvilket behov for opplæring krever rollen?
- Hva slags brukerstøtte har rollen behov for?

En ordremottaker må ha tilgang til en rekke verktøy for å kunne utføre sine arbeidsoppgaver. Fotograf: Science Photo Library

Hvis vi ser på rollene i eksemplet vårt, kan vi tenke oss at ordremottakerne vil trenge:

- en standard PC
- programvare for å registrere kunder og ordrer
- lese- og skrivetilgang til kunderegister og ordreregister
- opplæring i bruk av kunderegister og ordreregister
- vanlig brukerstøtte for PC
- telefonstøtte fra leverandøren av kunderegister og ordreregister

Lagersjefen trenger:

- en standard PC
- lese- og skrivetilgang til lagersystemet
- lesetilgang til kunderegisteret og ordreregisteret
- opplæring i bruk av lagersystemet
- vanlig brukerstøtte for PC

Lagermedarbeiderne kan antakeligvis dele på utstyret og trenger:

- en standard PC
- lesetilgang til ordreregisteret
- skriver for å skrive ut pakksedler

Legg merke til at ulike ansatte også kan ha behov for andre programmer og tilganger i forbindelse med andre arbeidsoppgaver. Men i denne sammenhengen vurderer vi bare hva som trengs for å fylle den enkelte rollen i den arbeidsprosessen vi ser på.

Når vi jobber med å vurdere IKT-støtte i arbeidsprosesser, kan det også dukke opp oppgaver som vi ikke tenkte på da vi kartla prosessen. I så fall må vi gå tilbake og sette de inn i et flytskjema. Vi kan for eksempel tenke oss at vi oppdager at ordremottakeren også må kunne skrive ut en ordrebekreftelse til kunden når bestillingen er registrert. Det vil igjen kreve at rollen som ordremottaker trenger en skriver.

Systemer som inngår som en del av prosessen, kalles for prosesskritiske. Det vil si at hele prosessen stopper opp hvis de ikke fungerer.

Kravdefinisjon og kravspesifikasjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kravdefinisjon og kravspesifikasjon (123591)

Når vi skal anskaffe utstyr eller programvare til en virksomhet, er det viktig å være tydelig på hvilke krav vi har til løsningen.

Når vi vet hvilke krav vi har til løsningen, blir det enklere for alle som er involvert. Brukerne vet hvilke muligheter systemet vil få. Leverandører vet hva de må levere, og virksomheten vet hvilke behov det vil være for driftsrutiner, opplæring og brukerstøtte.

Det gjør det også enklere å vurdere tilbud fra leverandører og beregne både anskaffelseskostnader og driftskostnader.

Krav til IKT-systemer kan beskrives enten som en **kravdefinisjon** eller som en **kravspesifikasjon**.

En kravdefinisjon er en brukerorientert beskrivelse av et IKT-system, mens en kravspesifikasjon er en presis teknisk beskrivelse av det samme systemet.

Kravdefinisjon

En kravdefinisjon skrives i vanlig språk slik at den er forståelig for alle som er involvert, og kravene deles inn i to kategorier: **funksjonelle** og **ikke-funksjonelle krav**.

Funksjonelle krav er en beskrivelse av hvordan systemet skal «oppføre» seg, hva det skal gjøre og ikke gjøre, tilgjenglighet, brukervennlighet og sikkerhet fra brukerens ståsted. Ofte brukes prosessflytdiagrammet for arbeidsprosessen som utgangspunkt for beskrivelsen. Legg også merke til at beskrivelsen må ta hensyn til at ulike roller i prosessen kan ha ulike krav til systemet.

Ikke-funksjonelle krav er rammene for systemet, for eksempel responstid, oppetid, ressursforbruk, antall samtidige brukere, og lignende. De ikke-funksjonelle kravene skiller seg fra de funksjonelle ved at det er mulig å tallfeste dem.

Det kan være en utfordring å skrive en kravdefinisjon som ikke har krav som kommer i konflikt med hverandre når alle roller skal ha med sine behov og ønsker. Dette gjelder spesielt for prosesskritiske systemer som har mange brukere. Ofte har også brukerne ønsker som det ikke er teknisk mulig å innfri med det utstyret eller programmet som er utgangspunkt for systemet.

Kravspesifikasjon

En kravspesifikasjon til et IKT-system er en teknisk beskrivelse av systemet, ofte presentert som datamodeller som viser tabellstruktur i en database og relasjoner mellom ulike datatyper. Kravspesifikasjoner er ikke beregnet på brukere av systemet, men for at systemutviklere skal ha en presis beskrivelse å forholde seg til.

En annen viktig informasjon i kravspesifikasjoner er **kryss-referanser** for kravene, slik at hvis et krav endres, kan man se hvilke andre krav som blir påvirket av endringen.

Gode og presise kravspesifikasjoner er viktige for å kunne beregne kostnader ved innkjøp av nye IKT-systemer. Fotograf: Berit Roald

Dersom bedriften skal ha et nytt lagersystem, bør det lages en kravspesifikasjon.

Oppgave

Tenk deg at du arbeider for en kjede som selger sportsklær og utstyr. Kjeden har behov for å oppdatere nettsidene sine, og du skal skrive en kravdefinisjon for disse sidene.

Oppgave

Selv om de to begrepene – kravdefinisjon og kravspesifikasjon – har ulik betydning, kan du nok oppleve en del sammenblanding. Ofte brukes betegnelsen kravspesifikasjon selv om det egentlig er snakk om en kravdefinisjon.

En kravdefinisjon er en brukerorientert beskrivelse av et IKT-system, mens en kravspesifikasjon er en presis teknisk beskrivelse av det samme systemet.

Skriv en kravdefinisjon for et dataspill som du kjenner godt.

Oppgaver

Flytskjema med iterasjon

Forfatter: Kjell Arild Welde
Flytskjema med iterasjon (134700)

Iterasjon betyr gjentakelse. Valg og gjentakelse er datamaskiner gode til. Ordremottak er en arbeidsprosess, men flytskjema kan også brukes på mer banale prosesser, som å krysse en vei. Dette er tema i denne oppgaven.

Du skal lage et flytskjema som viser hvilken informasjon en fotgjenger får, og hvilke valg han må ta, når han krysser en vei utenom en fotgjengerovergang.

Krav til oppgaven: Skjemaet kan lages i Creately eller et tilsvarende verktøy. Pilene skal gå i riktig retning, og valgene skal være merket med "Ja" og "Nei".

Alle prosesser og valgboksene skal ha navn. Skjemaet skal eksporteres.

Vareleveringsvirksomheten

Forfatter: Kjell Arild Welde
Vareleveringsvirksomheten (134702)

Et prosessflytdiagram er et diagram som viser stegene i en arbeidsprosess. Prosessflytdiagrammer kalles også for arbeidsflytdiagrammer eller bare flytskjema. I denne oppgaven skal du lage et flytskjema for en vareleveringsvirksomhet.

Kari, Mari og Per jobber i en virksomhet som selger varer. Kari jobber på sentralbordet. Det er hun som tar imot bestillingene. Varebestillingene kommer både via brev og over telefon, men de fleste kommer via e-post.

Det første Kari gjør når hun får en bestilling, er å sjekke om det er fra en tidligere kunde. Er det ikke det, skriver hun opp navn, adresse og poststed i kunderegisteret. Tidligere var kunderegisteret en skoeske med kort – ett kort for hver kunde. Men det er lenge siden. Nå skriver Kari inn kundeinfoen på en datamaskin.

Kommer bestillingen fra en kunde med kundenummer (altså en tidligere kunde), registrerer hun bestillingen. Bestillingen går til ordreregistret. Mari sjekker om varen er på lager. Er den ikke det, gir hun kunden beskjed og sender en bestilling til leverandøren.

Når virksomheten får varer fra grossisten (leverandøren), pakker Per opp kolliene med varer og setter dem inn i lagerhyllene, mens Mari oppdaterer lagersystemet.

Hvis de bestilte varene er på lager, skrives det ut en pakkseddel på bakgrunn av informasjonen som finnes i kunde- og ordreregistret. Per henter varene på lageret, pakker dem og sender pakken til kunden.

Oppgave 1 (liten)

I beskrivelsen står det: Nå skriver Kari inn kundeinfoen på en datamaskin.

Lag et flytskjema i Creately eller et annet tilsvarende verktøy som viser detaljert hva hun gjør når hun taster inn kundeinfo.

Oppgave 2 (stor)

Tegn et flytskjema over alle prosessene i virksomheten. Tegn også inn dataflyten.

Planlegging

Litt om prosjektorganisering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Litt om prosjektorganisering (119652)

Innføring av nye IKT-systemer i en virksomhet organiseres ofte som prosjekter, og IKT-systemer inngår ofte i andre prosjekter. Som IKT-medarbeider bør du derfor vite litt om prosjektorganisering.

Et prosjekt kjennetegnes ved at:

- oppgaven er ny og kan være ukjent for prosjektdeltakerne
- det er en engangsoppgave
- ressursene er begrenset
- det skal ferdigstilles innen en bestemt tidsfrist
- prosjektdeltakerne arbeider normalt ikke sammen

Nå er det ikke noe krav at alle disse kjennetegnene skal være oppfylt for at et arbeid skal kunne organiseres som et prosjekt. Det finnes en rekke definisjoner på hva et prosjekt er, og man kommer antakelig aldri til å bli enige om en endelig definisjon.

Fotograf: Anders Wiklund

Lenke:

- Scrum – Wikipedia

Prosjektorganisering blir ofte benyttet i forbindelse med utvikling av IKT-systemer, og det er lett å forstå hvorfor. Utvikling eller innføring av nye IKT-systemer vil i de fleste tilfeller være en **ny oppgave** for deltakerne. Det vil si: De kan godt ha deltatt i lignende prosjekter tidligere, men utviklingen av ett bestemt system vil være en ny oppgave.

Likeledes er det en **engangsoppgave**. Når systemet først er på plass og i drift, skal det ikke utvikles igjen. Ingen virksomheter har ubegrensede ressurser å legge i IKT-systemene sine, så **ressursene er begrenset**, og virksomhetene ønsker naturlig nok å få systemet på plass så snart som mulig. Når det gjelder det siste punktet, vil deltakerne i et IKT-utviklingsprosjekt nesten alltid inkludere **personer som normalt ikke arbeider sammen til daglig** – for eksempel folk fra ulike avdelinger som skal bruke systemet: IKT-medarbeidere, eksterne leverandører eller konsulenter.

Det finnes flere måter å organisere prosjekter på, men felles for de fleste er at de har en prosjektansvarlig eller prosjektleder og et antall prosjektdeltakere med spesifikke oppgaver. Det er også utviklet flere modeller spesifikt med tanke på organisering av IKT-prosjekter. En mye brukt løsning kalles Scrum.

Når en virksomhet skal innføre nytt IKT-system, blir innføringen ofte organisert som et prosjekt.

Hva er spesielt for IKT-prosjekter?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hva er spesielt for IKT-prosjekter? (119659)

I utgangspunktet er det ikke noen forskjell på IKT-prosjekter og andre prosjekter. Hovedtrekkene og arbeidsmetodene er de samme på alle vesentlige punkter, men IKT-prosjekter har også noen særtrekk som gjør at de kan skille seg fra andre prosjekter på enkelte områder.

Utviklingstakten for IKT er svært høy
Sammenliknet med de fleste andre fagområder går utviklingstakten for IKT med sjumilsstøvler. Det innbærer at det er svært krevende å holde seg oppdatert, og det kan være vanskelig å skaffe den nødvendige kompetansen til et IKT-prosjekt. Tidligere erfaring blir også mindre verdt når utviklingen har gått videre, og i noen tilfeller kan teknologien til og med endre seg mens prosjektet pågår.

Én årsak til at bedriften setter i gang IKT-prosjekter kan være et ønske om økt effektivitet i arbeidsprosessene.

Markedet endrer seg raskt
K r a v e t til IKT-løsninger er gjerne drevet av markedsbehovet og konkurransesituasjonen. Den høye utviklingstakten for teknologi fører også med seg raske og store endringer i markedet. Det gjør at IKT-prosjekter ofte kan være svært tidskritiske hvis man skal oppnå det ønskede resultat. Det hjelper ikke om man har gjennomført et vellykket prosjekt hvis markedet etterspør noe annet når man er ferdig.

Prosjektresultatet krever ofte omstillinger i virksomheten
Mange IKT-prosjekter har som mål å effektivisere eksisterende rutiner eller systemer, og det betyr at virksomheten ikke kan «fortsette som før» hvis de skal få fullt utbytte av prosjektresultatet. IKT-prosjekter griper derfor ofte inn i de ansattes arbeidsdag, slik at mange mennesker blir involvert.

Kravet til funksjonalitet er stadig økende
Utviklingstakten gjør også at brukere etterspør stadig flere og mer avanserte funksjoner. En faktor som svært ofte gjør seg gjeldende for IKT-prosjekter, er det som på engelsk kalles «scope creep». Scope creep er betegnelsen på det som skjer når et prosjekt vokser underveis – at man underveis får nye ideer og forslag til hva som bør inkluderes i det systemet man arbeider med, og at man inkluderer disse i prosjektet.

Scope creep kommer gjerne som en konsekvens av at kravdefinisjonene var for dårlige før prosjektet startet, eller av at man oppdaget nye muligheter underveis i utviklingen. Det siste er ikke uvanlig, for brukere har ofte ikke full forståelse for hva som er mulig å få til, eller oversikt over hva de faktisk trenger, før man er et godt stykke inne i prosjektet. Ofte vil ikke forslagene til nye funksjoner komme før det nye systemet testes av brukerne.

Selv om ideer som oppstår underveis, ofte tilhører kategorien «greit å ha», er de gjerne også fornuftige, og det kan være fristende å inkludere dem. Men hvis man vil ha noe håp om å fullføre prosjektet innenfor de rammene som er satt, bør man være svært streng med hensyn til hva man skal tillate av scope creep. Selv små endringer og tillegg kan kreve mye arbeid og dermed føre til at prosjektet går utover budsjett og tidsplan.

Den korrekte måten å håndtere scope creep på, er å samle alle forslag som kommer inn, og legge dem til ved neste oppdatering eller gjennomføre dem som et eget prosjekt seinere. Skikkelig planleggingsarbeid bidrar også i stor grad til å redusere antallet endringer når prosjektet først er startet.

Hvorfor IKT-prosjekter mislykkes

Forfatter: Arne Jansen
Hvorfor IKT-prosjekter mislykkes (119679)

Sammenlignet med andre prosjekter er det en overraskende stor andel IKT-prosjekter som mislykkes eller bare er delvis vellykket. Det vil si at man ikke oppnådde målene, man brukte lengre tid enn beregnet, eller det ble dyrere enn man så for seg.

Hvorfor IKT-prosjekter mislykkes?
Opphavsmann: Arne Jansen

Det kan være mange årsaker til at et prosjekt «mislykkes», men for IKT-prosjekter er det særlig følgende faktorer som peker seg ut:

For dårlige kravdefinisjoner
Uklare mål og krav er en av de viktigste årsakene til at IKT-prosjekter mislykkes. Når prosjektet ikke er klart nok definert på forhånd, reduseres mulighetene for suksess betraktelig. For eksempel er ikke resultatet tydelig nok definert når det er avvik mellom hva brukerne og ledelsen tror de vil få, og hva de som skal gjennomføre prosjektet, tror de skal levere.

IKT-prosjekter fokuserer ofte også for mye på teknologien og for lite på den oppgaven prosjektet skal løse. Det vil si at prosjektdeltakerne, og da særlig IKT-medarbeiderne, ikke har kunnskap nok om hva det nye systemet skal brukes til, og hvordan det vil bli brukt.

Urealistisk tidsplan
Mange IKT-prosjekter har en urealistisk tidsplan. Det er verdt å merke seg at for optimistiske anslag over hvor lang tid en oppgave vil ta, er én av de feilene IKT-medarbeidere oftest gjør når de planlegger prosjekter. Eksterne leverandører som ønsker å selge produktene sine, er gjerne også altfor optimistiske når det gjelder hvor lang tid det vil ta å utvikle, levere, installere og kjøre i gang et system.

For knappe ressurser
Hvis kostnadene eller behovet for andre ressurser blir høyere enn forventet, må prosjektet ofte avsluttes før det er ferdig. Dermed går investeringen tapt uten at virksomheten oppnår den gevinsten de så for seg.

Manglende kunnskaper eller feil kompetanse
Altfor mange prosjekter settes i gang uten at den nødvendige kunnskapen er på plass. IKT-medarbeidere gjør seg skyldige i å svare ja nå de blir spurt om de kan påta seg en oppgave som de egentlig ikke har tilstrekkelig fagkunnskap om. Man føler kanskje at man burde kunne gjøre det man blir spurt om, og antar at man underveis kan lære seg det man trenger, så man tar sjansen og sier ja.

I en del tilfeller har heller ikke virksomheten kartlagt hvilken kompetanse gjennomføringen av et prosjekt vil kreve før prosjektet startes. Man regner med at man kan skaffe den nødvendige kompetansen når det blir behov for den.

Manglende evne til å gjøre nødvendige omstillinger
IKT-prosjekter innebærer ofte at virksomheten må gjøre omstillinger i organisasjonen, rutinene eller andre systemer. Hvis ikke ledelsen eller de ansatte er innforstått med dette, kan prosjektet feile fordi man mangler evne eller vilje til å gjøre de omstillingene som er nødvendige for å lykkes.

I tillegg kan prosjekter også feile eller bli forsinket på grunn av

- for store forventninger til resultatet
- manglende styring og kontroll
- manglende deltakelse fra dem som skal bruke systemet
- endrede behov før prosjektet er ferdig

Artikler (eksterne lenker):

- Sved av hundrevis av millioner på mislykket IT-prosjekt
- Stopper IT-prosjekt til 160 millioner

> Uklare mål og krav er en av de viktigste årsakene til at IKT-prosjekter mislykkes.

Vellykkede IKT-prosjekter

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Vellykkede IKT-prosjekter (119687)

Nøkkelen til vellykkede IKT-prosjekter ligger i god planlegging og grundig oppfølging. Slurv i planleggingsarbeidet og manglende oppfølging og styring underveis fører nesten alltid til at prosjektet mislykkes.

Det er fem faktorer som er kritiske for at vi skal lykkes med et IKT-prosjekt:

Opphavsmann: Arne Jansen

Brukerne må involveres
Brukerne må inkluderes i prosjektplanleggingen helt fra starten av. Det viser seg også at det i mange tilfeller er positivt å ha en bruker – og ikke en IKT-medarbeider – som prosjektleder.

Prosjektdeltakerne må frigjøres fra andre oppgaver
Å arbeide på et prosjekt er ikke en deltidsjobb, og både IKT-medarbeidere og brukere har allerede andre oppgaver som fyller arbeidsdagen. Når et prosjekt starter, må deltakerne få frigjort den nødvendige tida som kreves for å jobbe med prosjektet.

Tilgang til riktig kompetanse
Mange IKT-prosjekter forutsetter spesialkunnskaper. Å forsøke å lære det man trenger, underveis, er en svært dårlig løsning. Når man har identifisert hvilke kunnskaper prosjektet krever, må man enten lære opp medarbeiderne før prosjektet settes i gang, eller leie inn nødvendig ekspertise.

Kunnskap om prosjektstyring
Å lede et IKT-prosjekt er en svært krevende oppgave, og prosjektet må styres av noen som har kunnskap og erfaring fra prosjektledelse. Ofte blir prosjektleder for et IKT-prosjekt valgt på bakgrunn av teknisk IKT-kompetanse, men dette er ikke noe godt kriterium. Selv om deltakerne i et IKT-prosjekt selvsagt må ha den nødvendige IKT-kompetansen, er ikke dette noe krav for å lede prosjektet. De viktigste egenskapene en prosjektleder må ha, er prosjekterfaring og gode kunnskaper om selve virksomheten.

Bruke en fastlagt prosjektmodell
Prosjektet bør organiseres etter en fastlagt prosjektmodell som alle deltakerne kjenner. Dette betyr at prosjektdeltakerne må få opplæring i den aktuelle prosjektmodellen før prosjektet startes.

Prosjektveiviseren
I 2009 lanserte Direktoratet for forvaltning og IKT en egen nettside kalt Prosjektveiviseren med en felles prosjektmodell for offentlig sektor. Hensikten er å samle gode erfaringer i en offentlig felles prosjektmodell som skal bidra til at flere offentlige IKT-prosjekter blir vellykket.

Artikler

- Prosjektveiviseren
- Vellykket IT-prosjekt

Nøkkelen til vellykkede IKT-prosjekter ligger i god planlegging og grundig oppfølging.

Innhente informasjon

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innhente informasjon (119694)

En viktig del av planleggingsarbeidet for nye IKT-systemer er å hente inn informasjon fra alle som på en eller annen måte blir involvert i eller påvirket av systemet.

En ny systemløsning involverer og påvirker vanligvis mange mennesker som kan ha ulike behov og forventninger til systemet. Det kan også være at ønsker og krav er i konflikt med hverandre, og det er viktig å avklare dette før man bestemmer seg for en løsning.

Informasjonen skal ofte danne grunnlag for en kravdefinisjon. Kravdefinisjonen er omtalt i kompetansemålet «Kartlegge behov for IKT-støtte i en arbeidsprosess og utarbeide en kravdefinisjon for et IKT-system».

De tre viktigste gruppene vi må innhente informasjon fra, er vanligvis ledelsen, brukerne og systemleverandørene, men det kan også være aktuelt å innhente informasjon fra kunder, konsulenter, brukerstøtter eller andre.

- **Ledelsen** har vanligvis klare mål for hva virksomheten skal oppnå med systemet, og bestemmer som regel også rammene for kostnader og tidsforbruk.
- **Brukerne** er de som kjenner arbeidsoppgavene best og vet hvilke problemer virksomheten har i dag, som systemet bør løse.

Å innhente god informasjon fra alle dem som skal bruke systemet, er svært viktig for å lykkes med et nytt IKT-system.

Vi forventer kanskje at ledelsen og brukerne er enige om hva et nytt system skal gjøre, og hvordan det skal fungere, men det er ikke alltid tilfellet. Ledelsen er vanligvis mest opptatt av hvilke fordeler systemet vil gi virksomheten. Brukerne på sin side er vanligvis mest opptatt av sin arbeidssituasjon og hvordan den blir påvirket. Dette er årsaken til at **arbeidsmiljøloven** stiller krav til at arbeidstakerne skal være med i utformingen av nye systemer.

Avhengig av hva slags system det er snakk om, kan det også være aktuelt å innhente informasjon fra kunder og brukerstøtte.

- **Kundene** kan si noe om hvordan virksomheten kan forbedre seg.
- **Brukerstøtten** kan si noe om hvilke problemer man har med eksisterende systemer.

Den innsamlede informasjon danner grunnlaget for å lage en kravdefinisjon som alle kan akseptere. Kravdefinisjonen brukes igjen som utgangspunkt for å innhente informasjon fra systemleverandører og eventuelle konsulenter.

- **Systemleverandørene** kjenner mulighetene og begrensningene for sine produkter.
- **Konsulentene** har gjerne erfaring med tilsvarende virksomheter eller systemer og vet hvilke feil andre har gjort tidligere.

En ny systemløsning involverer og påvirker vanligvis mange mennesker som kan ha ulike behov og forventninger til systemet.

Fokuser på virksomheten

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Fokuser på virksomheten (119696)

En vanlig feil IKT-medarbeidere gjør når de skal gi råd ved planlegging av nye systemløsninger, er at de fokuserer for mye på teknologien og for lite på virksomheten.

Når en virksomhet skal investere i en ny systemløsning, er det for å løse de arbeidsoppgavene de har, på en bedre og mer effektiv måte. Teknologien er i seg selv ikke viktig, og svært få virksomheter investerer i IKT for teknologiens skyld.

Spørsmålet er derfor ikke hvilket system som er best, men hvilket system som best løser virksomhetens oppgaver.

En investering i et nytt IKT-system må derfor alltid veies opp mot den nytteverdien systemet gir virksomheten, og i tillegg til teknologi må vi se på økonomi, kompleksitet og brukervennlighet.

Viktige spørsmål som må besvares, er:

- Vil systemet gjøre arbeidet mer effektivt?
- Vil systemet redusere kostnadene for virksomheten?
- Oppnår virksomheten noen form for konkurransefordel ved å ta i bruk systemet?
- Hvor lang tid vil det ta før effektiviseringen eller konkurransefordelen har tjent inn kostnadene?
- Hvor store drifts- og vedlikeholdskostnader fører systemet med seg?
- Hvilke omstillinger og endringer i rutiner må virksomheten gjøre på grunn av systemet?
- Hvilket behov for opplæring krever systemet?

Dersom du for eksempel er IKT-medarbeider i en lagervirksomhet, bør du sette deg nøye inn i hvilke arbeidsoppgaver de ansatte skal utføre, før du begynner på arbeidet med å lage en kravdefinisjon for et nytt IKT-system.

For å kunne svare på disse spørsmålene er det ikke tilstrekkelig å ha IKT-kompetanse. Du må også forstå hvordan virksomheten fungerer, og vite hvilke oppgaver de ansatte som skal bruke systemet, har.

Spørsmålet er ikke hvilket system som er best, men hvilket system som best løser virksomhetens oppgaver.

Anskaffelser

Lover og regler når et nytt system skal tas i bruk

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Lover og regler når et nytt system skal tas i bruk (119703)

Både ledelsen og de ansatte i virksomheten kan ha ønsker for en ny systemløsning som kommer i konflikt med lover og regler. Vi må derfor nøye vurdere om et nytt IKT-system gjør at virksomheten bryter noen regler eller åpner for misbruk.

Lover og regler for IKT er grundig omtalt i faget «Bruker- og driftsstøtte» i kompetansemålene «*Behandle fortrolige opplysninger på en etisk forsvarlig måte innenfor rammene av gjeldende regelverk*» og «*Gi råd i henhold til gjeldende regelverk ved anskaffelse, bruk og utvikling av IKT-systemer*».

Vi oppsummerer kort de lover og regler vi må vurdere:

- personvern: personopplysningsloven og personopplysningsforskriften
- arbeidsmiljøloven
- krav til universell utforming av IKT
- åndsverkloven

Personvern

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Personvern (119705)

Personvern er retten til et privatliv og retten til å bestemme over egne personopplysninger. Før vi tar i bruk et nytt IKT-system, må vi forsikre oss om at systemet tar vare på personopplysninger på en forsvarlig måte, slik at de ikke kommer på avveie eller kan misbrukes.

Det er flere lover som gjelder personvern. De viktigste er personopplysningsloven og personopplysningsforskriften. Loven slår fast prinsippene for hva som er lov, og hva som ikke er lov, og forskriften forklarer hvordan reglene skal gjennomføres i praksis.

Noen bransjer og yrkesgrupper har også egne lover og regler som må følges. Eksempler på slike lover er helseregisterloven og regler om taushetsplikt.

Hvis en ny systemløsning skal brukes til å registrere personinformasjon, må vi forsikre oss om at systemet oppfyller kravene i personopplysningsloven før det settes i drift.

Reglene for taushetsplikt er strenge, blant annet når det gjelder behandling av helseinformasjon.

Viktig spørsmål er:

- Hvilke personopplysninger blir registrert i systemet?
- Hvem skal registrere personopplysninger i systemet?
- Hvem får tilgang til personopplysningene?
- Hvordan blir personopplysninger lagret og beskyttet?
- Hvordan skal forespørsler om innsyn følges opp?
- Hvilke rutiner for retting og sletting av personopplysninger kreves?
- Må det sendes melding til Datatilsynet før systemet tas i bruk?

Et personregister kan også kreve konsesjon fra Datatilsynet. Det gjelder blant annet hvis noen av opplysningene som skal registreres i systemet, er sensitive.

Lenker:

- personopplysningsloven
- personopplysningsforskriften

Før vi tar i bruk et nytt IKT-system, må vi forsikre oss om at systemet tar vare på personopplysninger på en forsvarlig måte, slik at de ikke kommer på avveie eller kan misbrukes.

Arbeidsmiljø

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Arbeidsmiljø (119707)

En ny systemløsning kan ikke settes i drift uten at brukerne er blitt informert og har fått nødvendig opplæring.

Arbeidsmiljøloven § 4-2 sier at arbeidstakere skal bli løpende informert om systemer som brukes i arbeidet. De skal få nødvendig opplæring i bruk av systemene og være med på utformingen av dem.

Paragrafen setter fem krav:

1. Det skal legges til rette for at arbeidstakeren får mulighet til å utvikle seg faglig og personlig gjennom sitt arbeide.
2. Arbeidet skal organiseres og tilrettelegges med hensyn til den enkeltes arbeidsevne, kunnskaper, alder og andre forutsetninger.
3. Det skal legges vekt på å gi arbeidstakeren mulighet til selvbestemmelse, innflytelse og faglig ansvar.
4. Arbeidstakeren skal få mulighet til variasjon i arbeidet og til å se sammenhengen mellom enkeltoppgaver.
5. Virksomheten skal gi nok informasjon og opplæring til at arbeidstakeren klarer å utføre arbeidet når det skjer endringer i vedkommendes arbeidssituasjon.

I praksis betyr dette at når en virksomhet innfører et nytt IKT-system, må de informere de ansatte på forhånd og gi alle som blir berørt av endringene, mulighet til å uttale seg. Men systemet må ha betydning for hvordan den enkelte skal gjøre jobben sin før loven er aktuell. Vanlige oppgraderinger av programmer og lignende er ikke nok.

Når et nytt system skal tas i bruk, må de som skal bruke det, også få nok opplæring til at de klarer å gjøre jobben og forstå hva det er de gjør.

Virksomheten må også ta hensyn til forutsetningene de enkelte medarbeiderne har. For eksempel må en virksomhet som innfører et nytt, avansert system som skal brukes av personer med liten eller ingen erfaring med IKT fra før, naturlig nok gi mye opplæring.

Når bedriften planlegger å innføre et nytt IKT-system, skal de ansatte informeres og få mulighet til å uttale seg.

Lenke:

- arbeidsmiljøloven

Når en virksomhet innfører et nytt IKT-system, må den informere de ansatte på forhånd og gi alle som blir berørt av endringene, mulighet til å uttale seg.

Universell utforming av IKT

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Universell utforming av IKT (119712)

Universell utforming av IKT handler om å utforme IKT-løsninger slik at de kan brukes av alle, uavhengig av funksjonsnivå.

At noe er universelt utformet, vil si at det skal kunne brukes av alle selv om de har en funksjonshemning. Det kan være alle typer bevegelseshemninger, men også dårlig syn eller dårlig hørsel.

Talesyntese der tekst på nettsider leses opp for brukeren, er ett av flere tiltak for å gjøre innhold på nettsider tilgjengelig for blinde og svaksynte.

Lenke:

- Universell utforming av IKT

Universell utforming av IKT / fagstoff

http://ndla.no/nb/node/119712

Fornyings-, administrasjons- og kirkedepartementet har utarbeidet en forskrift med krav til universell utforming av IKT-løsninger. Planen er at kravene skal bli lovpålagt fra 2013, men innholdet i kravene blir ikke endelig kjent før forskriften trer i kraft.

I første omgang skal reglene om universell utforming gjelde for nettløsninger og automater, slik at alle skal kunne bruke dem. Dette gjelder for eksempel billettautomater, minibanker, netthandelssider, nettsider med informasjon til allmennheten og lignende.

Sosiale media som blogger, Facebook, Twitter og andre tjenester som brukes i privat sammenheng, er foreløpig holdt utenfor. Det er heller ikke meningen at kravene skal gjelde for interne systemer i virksomheter. Men hvis den nye systemløsningen i bedriften er ment for allmennheten, må de ta hensyn til universell utforming.

Hvis nye systemløsninger er ment for allmennheten, må de ta hensyn til universell utforming.

Åndsverkloven

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Åndsverkloven (119714)

Åndsverkloven sier at alle former for kopiering og nedlasting av rettighetsbeskyttet materiale er forbudt når man er klar over eller burde ha forstå at materialet er gjort tilgjengelig på ulovlig vis.

Stortinget vedtok våren 2005 endringer i åndsverkloven som gjorde alle former for kopiering og nedlasting av rettighetsbeskyttet materiale forbudt når man er klar over, eller burde ha forstått, at materialet er gjort tilgjengelig på ulovlig vis (såkalt piratkopiering). Dette inkluderer musikk, film, tekster (bøker), bilder og programvare.

Når virksomheten tar i bruk en ny systemløsning, må den passe på at den har gyldige lisenser for programvaren, og at systemet ikke inneholder rettighetsbelagt materiale som det ikke er betalt avgift for.

Pass på at du alltid benytter lovlig nedlasting av musikkfiler fra Internett. Ulovlig nedlasting medfører at musikeren ikke får betalt for arbeidet sitt.

Lenke:

- åndsverkloven

Brukerundersøkelse

Undersøke brukertilfredshet

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Undersøke brukertilfredshet (124570)

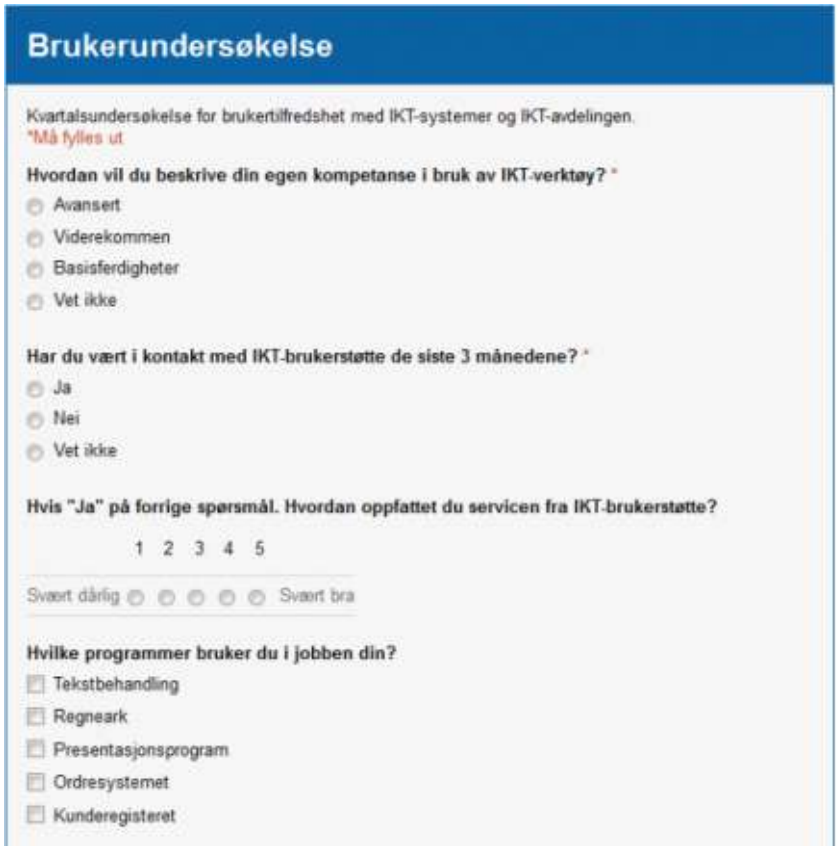
Selv om vi kan synes at både systemene og brukerstøtten fungerer som de skal, er det ikke sikkert at brukerne er av samme oppfatning. Vi må derfor regelmessig undersøke om brukerne er fornøyd.

I tillegg til å kontrollere at brukerne er fornøyd, er det å undersøke brukertilfredshet også viktig for å oppdage eventuelle områder der det har skjedd endringer som gjør at vi må forbedre oss.

Den enkleste måten å undersøke brukertilfredshet på er å bruke et nettbasert spørreskjema. Det finnes flere leverandører som tilbyr tjenester for dette. Noen eksempler er QuestBack, Enalyzer og SurveyMonkey. Disse tilbyr komplette verktøy for å lage, gjennomføre og analysere resultatene av undersøkelser.

Et annet alternativ er skjemafunksjonen i Google Dokumenter (Google Disk), som også kan brukes til å lage og gjennomføre enkle undersøkelser. Google skjema har også noen innebygde funksjoner for analyser, og resultatene kan eksporteres til Excel eller Google regneark for videre behandling der.

Eksempel på Google Disk spørreskjema.



Brukerundersøkelse

Kvartalsundersøkelse for brukertilfredshet med IKT-systemer og IKT-avdelingen.
*Må fylles ut

Hvordan vil du beskrive din egen kompetanse i bruk av IKT-verktøy? *

- Avansert
- Viderekommen
- Basisferdigheter
- Vet ikke

Har du vært i kontakt med IKT-brukerstøtte de siste 3 månedene? *

- Ja
- Nei
- Vet ikke

Hvis "Ja" på forrige spørsmål. Hvordan oppfattet du servicen fra IKT-brukerstøtte?

1 2 3 4 5

Svært dårlig ○ ○ ○ ○ ○ Svært bra

Hvilke programmer bruker du i jobben din?

- Tekstbehandling
- Regneark
- Presentasjonsprogram
- Ordresystemet
- Kunderegisteret

Brukerundersøkelse.

Opphavsmann: Google

Automatisert brukerundersøkelse

En del helpdeskprogram og system for registrering av brukerstøtte har funksjonalitet for automatisert innhenting av tilbakemelding fra brukerne.

Så snart en henvendelse er registrert som avsluttet i systemet, blir det automatisk sendt en e-post til brukeren eller kunden. Illustrasjonen under viser eksempel på en slik e-post.

Til: Arne Jansen
Emne: Feedback Service Desk

Kjære kunde

Din/deres henvendelse **CHG-129555** har nettopp blitt ferdigbehandlet og du har mottatt en sluttrapport på saken.

Vi er opptatt av at du skal være fornøyd med vårt supportapparat og at servicen svarer til forventningene.

For å forbedre oss er vi avhengige av tilbakemeldinger og håper derfor du kan sette av noen sekunder til å svare på 6 spørsmål om hvordan du opplevde håndteringen av din henvendelse.

Vi vil gjerne ha både ros og ris og oppfordrer deg til å være så ærlig som mulig!

Du besvarer spørsmålene ved å følge denne linken:

https://www.******.com/feedback/SoundingsSVN/survey.cfm?id=ED8255A7-B46C-9681-F6F13C22A742A940

Vennlig hilsen
Service Desk

Eksempel på automatisk utsendt spørreskjema fra helpdesk.

Opphavsmann: Arne Jansen

Når brukeren klikker på lenken i e-posten, vises et enkelt spørreskjema som i illustrasjonen under.

Eksempel på spørsmål i supportundersøkelse.

Opphavsmann: Arne Jansen

Ved å automatisere innhenting av informasjon på denne måten kan systemet kontinuerlig overvåke brukertilfredsheten og varsle så snart den faller under et nivå som er bestemt på forhånd.

Når brukerne får spørsmålene med en gang, mens opplevelsen fortsatt er fersk i minnet, er det også større sannsynlighet for at de svarer.

Ulempen er at undersøkelsen bare fanger opp dem som har fått saken sin løst. Systemet kan dermed vise at de fleste brukerne er fornøyd, mens det i virkeligheten er mange som er misfornøyd fordi saken deres ikke er løst og dermed står som åpen i systemet.

Den enkleste måten å undersøke brukertilfredshet på er å bruke et nettbasert spørreskjema.

Utforme spørreskjema

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Utforme spørreskjema (124571)

Tilsynelatende er det ganske enkelt å lage et spørreskjema, men det finnes mange mulige feller. Disse bør du forsøke å unngå.

Det første du må bestemme, er hva det er du skal undersøke, og hva du skal bruke resultatet til. Det har ingen hensikt å gjennomføre en undersøkelse bare for undersøkelsens egen skyld. Resultatet må føre til handling eller gi informasjon som kan brukes til planlegging eller til å ta avgjørelser.

Når du lager et spørreskjema, bør du innlede med å forklare hvorfor undersøkelsen blir gjennomført, og hva resultatet skal brukes til, slik at brukerne ser hensikten med å svare.

Antall spørsmål i spørreskjemaet bør begrenses til det absolutt nødvendige. Jo flere spørsmål en undersøkelse består av, jo færre svar får du. Det er også en risiko for at brukeren etter hvert begynner å klikke på tilfeldige svaralternativ bare for å bli ferdig med undersøkelsen.

Alle spørsmål må derfor vurderes grundig, og bare de som er viktige og nødvendige, skal være med. Hvis du ikke er helt sikker på hvorfor du stiller et spørsmål, eller hva du skal bruke svarene til, bør ikke spørsmålet være med.

Samtidig må du selvfølgelig være sikker på at du ikke mangler noen spørsmål som er vesentlige for å kunne bruke resultatet av undersøkelsen. For å finne ut om det er spørsmål som mangler, er det lurt å sette opp en oversikt over hvordan resultatene av undersøkelsen skal analyseres, *før* du sender ut spørreskjemaet. Da ser du raskt hvilke data du må ha for gjøre analysene, og om det er data du egentlig ikke trenger.

Når du lager et spørreskjema, bør du innlede med å forklare hvorfor undersøkelsen blir gjennomført, og hva resultatet skal brukes til, slik at brukerne ser hensikten med å svare.
Opphavsmann: Shutterstock

Formulere spørsmål

Spørsmålene i spørreskjemaet må formuleres slik at leseren ikke blir i tvil om hva det er du spør om, og du bør unngå ord og uttrykk som brukeren kanskje ikke forstår . Tenk på at det ikke er alle brukere som er kjent med faguttrykk som du tar for gitt.

At spørsmålet ikke bør kunne misforstås, er svært viktig, ellers risikerer du at brukeren egentlig svarer på noe annet enn det du spør om og gjerne vil ha svar på.

Eksempel

Å formulere spørsmål som ikke kan misforstås, kan være vanskeligere enn det høres ut som. Tenk deg for eksempel at du gjerne vil vite hvor mange som har hatt tekniske problemer med maskinen det siste kvartalet, og tar med spørsmålet:

”*Har du hatt tekniske problemer med maskinen de siste tre månedene?"* JA/NEI

Dette burde jo være et uproblematisk spørsmål, men det er slett ikke sikkert at alle brukerne klarer å skille mellom tekniske maskinproblemer, programvareproblemer og nettverksproblemer. For mange vil ethvert problem som har med IKT å gjøre, være av teknisk art. Dermed risikerer du å få et resultat som viser at det har vært store maskintekniske problemer, mens det i virkeligheten kanskje har vært problemer med et program som mange bruker.

Noen flere råd om spørsmål

- **Still ett spørsmål om gangen**. Unngå spørsmål der brukeren må ta stilling til flere ting. Hvis du for eksempel stiller spørsmålet:*"Er du fornøyd med responstid og kompetanse når du henvender deg til brukerstøtte?"* kan brukerne bli i tvil om hva de skal svare hvis de er fornøyd med kompetansen, men ikke med responstiden.

- **Unngå ledende spørsmål.** Ledende spørsmål er spørsmål der "riktig" svar er lagt inn i spørsmålet. Noen spørsmål er så opplagt ledende at de fleste klarer å unngå dem, som for eksempel: "*Er du fornøyd med den raske responstiden når du kontakter brukerstøtte?*"

  Men ikke alle ledende spørsmål er like opplagte. Tenk deg at du i en brukerundersøkelse gjerne vil finne ut hvor mange som trenger en ny datamaskin i løpet av det neste året. Hvis du stiller spørsmålet: "*Ønsker du deg en kraftigere datamaskin til neste år?*" vil undersøkelsen antakelig vise at nesten alle trenger en ny datamaskin. Spørsmålet er ledende fordi de fleste jo gjerne vil ha en kraftigere datamaskin, enten de trenger det eller ikke.

- **Gi alltid brukeren en mulighet til å skrive inn en egen kommentar.**Alle spørreskjema bør avsluttes med et fritekstfelt der brukeren kan skrive om det er noe han gjerne vil gjøre deg oppmerksom på, for eksempel at vedkommende er nyansatt og derfor ikke har nok erfaring til å svare på de spørsmålene du stiller.

Spørsmålene i spørreskjemaet må formuleres slik at leseren ikke blir i tvil om hva det er du spør om.

Spørsmålstyper

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Spørsmålstyper (124572)

Når du lager et spørreskjema, må du også bestemme hvordan spørsmålene skal besvares. Det gjør du ved å velge spørsmålstype. Du bør alltid forsøke å gjøre det så enkelt og raskt som mulig for brukerne å svare.

De mest brukte spørsmålstypene er:

- envalg
- flervalg
- skala
- tekst

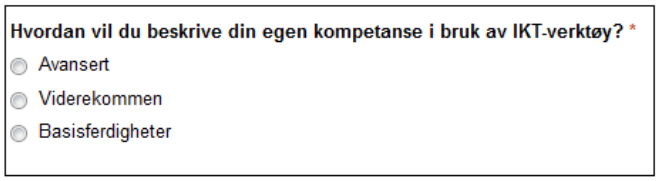
Det finnes flere andre spørsmålstyper, men de fleste av dem er bare varianter av de fire mest brukte, for eksempel envalgsspørsmål der man velger fra en nedtrekksmeny istedenfor å klikke på en knapp.

Envalg og flervalg

Envalgsspørsmål er spørsmål der brukeren bare kan velge ett av flere alternative svar, mens flervalgsspørsmål er spørsmål der det er mulig å velge flere svar.

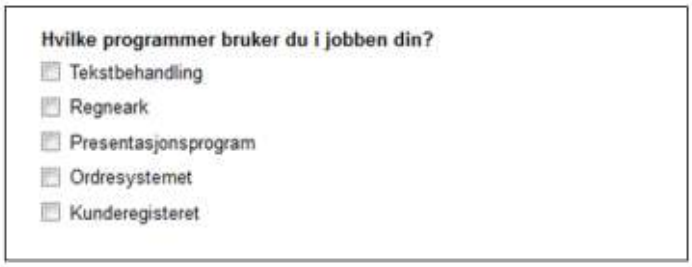
Envalgsspørsmål vises med radioknapper (sirkler), mens flervalgsspørsmål vises med avkryssingsbokser.

Eksempel på envalgsspørsmål:



Opphavsmann: Arne Jansen

Eksempel på flervalgsspørsmål:



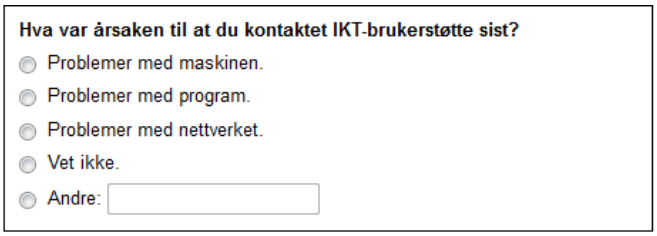
Opphavsmann: Arne Jansen

For envalgsspørsmål er det viktig at svaralternativene utelukker hverandre, slik at brukeren ikke opplever at flere av alternativene kan være riktige.

I noen tilfeller kan det være brukere som ikke er enig i noen av svaralternativene, ikke vet hva de skal velge, eller ikke ønsker å svare på spørsmålet. Slike spørsmål bør ha et eget ”null”- eller ”vet ikke”-alternativ. Det kan også være lurt å gi brukeren mulighet til å legge til et eget alternativ.

Generelt gjelder regelen at envalgsspørsmål alltid bør ha et ”vet ikke”-alternativ.

Eksempel på envalgsspørsmål med ”vet ikke”-alternativ og mulighet for å legge til et eget alternativ (Andre).



Opphavsmann: Arne Jansen

Skalaspørsmål

I skalaspørsmål blir brukeren bedt om å gi en vurdering basert på en forhåndsbestemt skala.

Alternativene på skalaen bør vanligvis være oddetall (3, 5 eller 7). Årsaken er at det på en skala med oddetall alltid vil være et valg i midten av skalaen. Dette vil bli oppfattet som nøytralt av brukere som er usikre på hva de skal svare, og fungere som et ”vet ikke”-alternativ.

Unntaket er når du ønsker å tvinge brukerne til å ta stilling den ene eller den andre veien. Da bør antall alternativer være et partall (2, 4, 6 eller 8), slik at det ikke finnes noe nøytralt alternativ i midten.

Eksempel på skalaspørsmål med fem alternativer.

Opphavsmann: Arne Jansen

Ikke bruk en lengre skala enn nødvendig. Færre alternativer gjør det enklere for brukeren å velge. I eksemplet over er det brukt en skala fra 1 til 5. Vi kunne også tenke oss den samme undersøkelsen med bare tre alternativer, siden det vi ønsker å finne ut, er om brukerne er fornøyd, misfornøyd eller et sted midt imellom.

Eksempel på skalaspørsmål med tre alternativer.

Opphavsmann: Arne Jansen

Men det er ikke sikkert at skalaen med tre alternativer ville gitt et like riktig bilde av situasjonen. Mange kvier seg for å velge de ytterste alternativene på et skalaspørsmål, og med bare tre alternativer vil flere være tilbøyelig til å velge alternativet i midten selv om de egentlig er litt misfornøyd eller ganske fornøyd. Med fem alternativer får brukeren mulighet til å si at de er litt misfornøyd eller stort sett fornøyd, ved å velge alternativ 2 eller 4.

Tekstspørsmål

Tekstspørsmål er spørsmål der brukeren må skrive et svar. Dette tar lengre tid og krever mer av brukeren. Tekstspørsmål bør derfor helst ikke være obligatoriske, og hvis det er mulig, bør du unngå dem. Unntaket er muligheten brukeren bør få til å gi egne kommentarer.

Eksempel på tekstspørsmål.

Opphavsmann: Arne Jansen

Generelt gjelder regelen at envalgsspørsmål alltid bør ha et ”vet ikke”-alternativ, og at skalaspørsmål bør ha et nøytralt alternativ i midten.

Gjennomføre undersøkelsen

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Gjennomføre undersøkelsen (124582)

Selv om du har fulgt alle råd, kan du ikke regne med at alle svarer på en brukerundersøkelse, men du kan øke antallet ved å gjøre det så enkelt som mulig å svare.

Som nevnt tidligere bør en undersøkelse ha så få spørsmål som mulig. Færre spørsmål gjør at flere svarer. Hvis du må gjennomføre en undersøkelse med mer enn ti spørsmål, bør du i starten fortelle brukeren hvor mange spørsmål det er, og hvor lang tid det vil ta å besvare dem.

Undersøkelser bør være anonyme. Så langt det er mulig, bør brukerundersøkelser være anonyme. Hvis brukeren tror at han eller hun kan bli identifisert, kan det påvirke svarene. Mange vil være tilbakeholdne med kritikk fordi de ikke har lyst til å bli sett på som noen som bare klager, eller de er redde for at det kan få negative konsekvenser for dem å svare på spørsmålene. Et unntak er selvsagt hvis undersøkelsen blir gjennomført for å kunne følge opp den enkelte brukeren individuelt.

Velg et tidspunkt da brukerne er til stede og har mulighet til å svare. Det er ikke alle dager eller tidspunkter som er like godt egnet for å sende ut en spørreundersøkelse. Fredag ettermiddag eller midt i sommerferien er for eksempel dårlige tidspunkter fordi mange ikke er til stede eller har annet å gjøre. Du bør også unngå perioder da du vet det er spesielt travelt eller midt i høysesongen for sesongbransjer.

Sjekk at skjemaet fungerer på alle typer maskiner. Hvis du ikke er sikker på hva slags maskiner brukerne har, må du sjekke at skjemaet fungerer på de mest brukte maskintypene. Det inkluderer også nettbrett og smarttelefoner.

Test spørreskjemaet før du starter undersøkelsen. Selv om du mener at du har fulgt alle råd og regler, kan det alltid ha sneket seg inn feil som du ikke har oppdaget eller tenkt på. Derfor er det lurt å sende skjemaet til noen utvalgte brukere som kan gi deg tilbakemelding før du sender undersøkelsen til alle.

Velg tidspunktet for gjennomføring av spørreundersøkelsen din med omhu. Det er for eksempel en dårlig idé å be en regnskapsfører om å besvare en brukerundersøkelse midt i årsoppgjøret.

Det har liten hensikt å sende en undersøkelse til brukere som ikke har noen forutsetning for å svare på spørsmålene.

Tenk på hvem undersøkelsen skal sendes til. Det har liten hensikt å sende en undersøkelse til brukere som ikke har noen forutsetning for å svare på spørsmålene. Sannsynligvis vil de ikke svare, men i verste fall besvarer de undersøkelsen og påvirker resultatet på en slik måte at undersøkelsen i praksis blir verdiløs. Husk at kvaliteten på svarene alltid er viktigere enn antallet svar.

Husk å gi tilbakemelding. Hvis det er mulig, bør de som svarer på en undersøkelse, alltid få en tilbakemelding. I anonyme undersøkelser kan det av og til være et problem, men de fleste verktøy for å lage og distribuere spørreundersøkelser har mulighet for å gi en automatisert bekreftelse når brukeren sender svaret. Her er det vanligvis også mulighet for å legge inn en takk for at de tok seg tid til å svare.

Lenke: Hvordan gjennomføre gode spørreundersøkelser på nett?

Så langt det er mulig, bør brukerundersøkelser være anonyme. Hvis brukeren tror at han eller hun kan bli identifisert, kan det påvirke svarene.

Analysere resultatene av undersøkelsen

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Analysere resultatene av undersøkelsen (124589)

Når undersøkelsen er gjennomført, må resultatene analyseres. Det har ingen hensikt å gjennomføre en brukerundersøkelse hvis det ikke fører til handling.

Resultatene av en undersøkelse bør alltid måles mot noe. Hvis det er gjennomført tilsvarende undersøkelser tidligere, er det naturlig å sammenligne med resultatene fra disse for å se om det er en positiv eller negativ utvikling. En annen mulighet er å tallfeste mål før undersøkelsen gjennomføres, og sammenligne resultatene med målene.

De fleste tjenester for nettbaserte spørreskjema inneholder egne analysemoduler. Ellers er regneark som Excel godt egnet som verktøy for å behandle og analysere resultater av spørreundersøkelser. Blant annet kan resultatene visualiseres ved hjelp av diagram.

Å tolke resultatene fra en undersøkelse er ikke alltid så enkelt, og det er lett å fokusere ensidig på avvik og negative resultater, eller omvendt. Det er viktig å spørre seg selv om det kan være feil i undersøkelsen, eller faktorer som har påvirket svarene, hvis vi får tall som avviker svært mye fra forventningene eller tilsvarende tidligere undersøkelser.

En hendelse like i forkant av en undersøkelse kan gi store utslag som ikke er representative for hva brukerne vanligvis mener. Hvis nettverket for eksempel har vært nede hele formiddagen den dagen du sender ut undersøkelsen, vil det antakelig påvirke resultatet i negativ retning selv om det kanskje er snakk om en engangshendelse. Svarene blir påvirket av stemningen den dagen.

Krysstabeller

I de fleste tilfeller vil det være aktuelt å ”koble” to eller flere spørsmål når vi skal analysere resultatene. Dette kalles å krysskoble eller krysstabulere. Excel har et eget verktøy for krysstabulering.

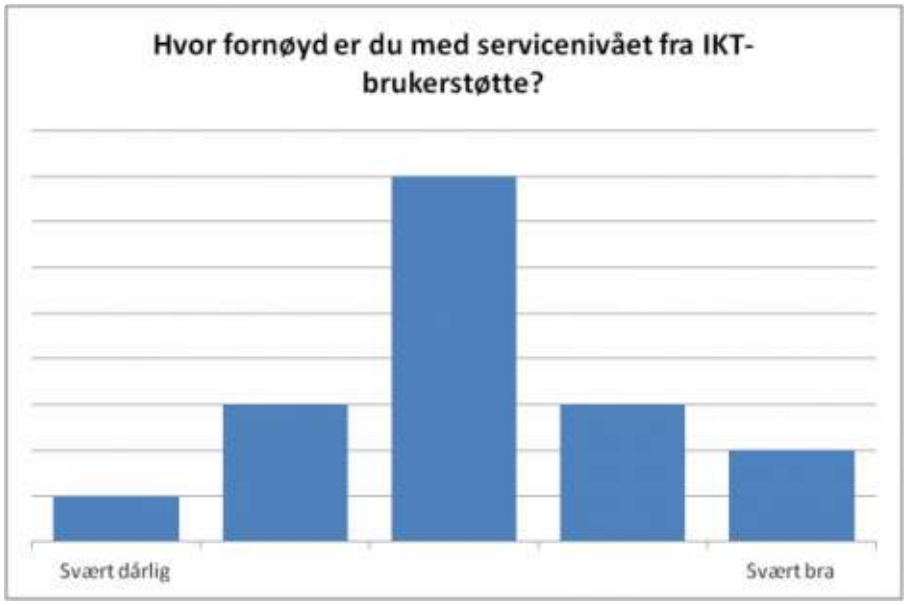
Krysstabulering gjør at vi kan oppdage ”skjulte” resultater i en undersøkelse. Tenk deg at du har gjennomført en undersøkelse der du blant annet har fått svar på følgende to spørsmål:

1. Hvordan vil du beskrive din egen kompetanse i bruk av IKT-verktøy?
    a. Avansert
    b. Viderekommen
    c. Basisferdigheter
2. På en skala fra 1 til 5, hvor fornøyd er du med servicenivået fra IKT-brukerstøtte?

Svarene på disse spørsmålene er selvsagt interessante hver for seg. Spørsmål 1 gir oss fordelingen av brukerkompetanse, noe som for eksempel kan være nyttig når vi skal planlegge opplæring.

Grafisk framstilling av svarfordeling.
Opphavsmann: Arne Jansen

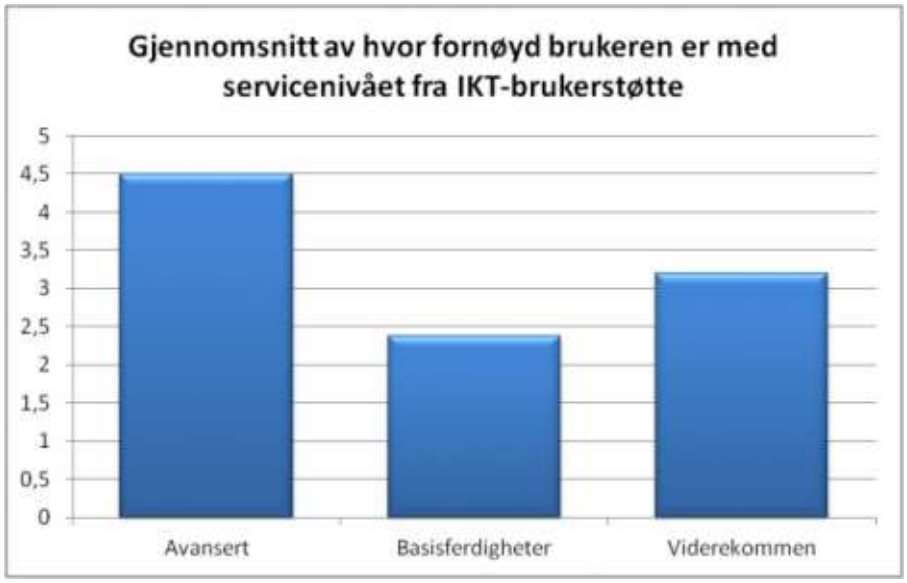
Svarene på spørsmål 2 forteller oss hvor godt fornøyd brukerne er med servicenivået, noe vi naturlig nok også er interessert i å følge med på.



Grafisk framstilling av svarfordeling.
Opphavsmann: Arne Jansen

Ved å koble de to spørsmålene sammen i en krysstabell kan vi i tillegg finne ut om det er forskjeller i hvordan brukere med ulik kompetanse oppfatter servicenivået.

Radetiketter	Gjennomsnitt av Hvor fornøyd er du med servicenivået fra IKT-brukerstøtte?
Avansert	4,50
Basisferdigheter	2,38
Viderekommen	3,20



Grafisk framstilling av resultater for en krysstabell.

Opphavsmann: Arne Jansen

Nå ser vi at brukerne med basisferdigheter er vesentlig mindre fornøyd enn de viderekomne og avanserte brukerne. Så må vi selvsagt finne ut hva som er årsaken, og hva som kan gjøres for å bedre resultatet, men hvis ikke vi hadde koblet sammen svarene fra de to spørsmålene, ville vi ikke ha visst at dette var situasjonen.

Å se på svarfordeling og sette opp enkle krysstabeller kan gi nyttig og viktig informasjon, men du bør være forsiktig med å trekke for bastante konklusjoner av resultatene fra en spørreundersøkelse.

Å gjøre korrekte analyser krever kunnskap om statistikk, matematikk og metode, blant annet beregning av feilmargin, konfidensnivå, standardavvik og statistisk signifikans. Dette er ikke en del av kompetansemålet i Virksomhetsstøtte, men nettsiden Spørreundersøkelser.no har en egen seksjon som forklarer de viktigste prinsippene. Her finnes det også en kalkulator for å beregne feilmarginen i spørreundersøkelser.

Lenke: Eksempel på analyse av brukerundersøkelse ved Universitetet i Bergen.

Vær forsiktig med å trekke for bastante konklusjoner av resultatene fra en undersøkelse.

Oppgaver

Brukerundersøkelse

Forfatter: Jan Frode Lindsø
Brukerundersøkelse (132382)

Her skal du gjennomføre en undersøkelse av brukertilfredsheten i en virksomhet for å få tilbakemeldinger som kan brukes til kontinulerlig forbedring.

Brukerundersøkelser kan være nyttige for å få tilbakemeldinger fra et større antall personer. I denne oppgaven bør dere jobbe sammen i grupper på 3-4 personer.

Ta kontakt med ledelsen på skolen, eller en annen oppdragsgiver som kan ha interesse av å få gjennomført en spørreundersøkelse for et bestemt formål. Dersom du gjennomfører den for skolen, kan man for eksempel lage brukerundersøkelser for skolekantinen, biblioteket, resepsjonen, IKT-brukerstøtte eller tilsvarende funksjoner. Man kan også lage spørreundersøkelser for å for eksempel kartlegge IKT-bruken i klasserommet.

Denne oppgaven gjennomføres som et prosjekt, og gjennomføring bør bestå av følgende prosesser:

1. Gå i grupper på 3-4 personer
2. Finn oppdragsgiver (for eksempel skoleledelsen)
3. Bestem tema/brukergruppe i samråd med oppdragsgiver
4. Sett opp spørreundersøkelsen
5. Distributer spørreundersøkelsen
6. Samle inn og analyser resultatet
7. Presenter resultatet for oppdragsgiver

Kontorstøttesystemer

Hva er kontorstøttesystemer?

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Hva er kontorstøttesystemer? (120167)

Kontorstøttesystemer er en samlebetegnelse på programvare for vanlige kontoroppgaver. Det inkluderer typiske Office-programmer som tekstbehandling, regneark og presentasjonsprogram, men mange andre typer programmer kan også regnes som kontorstøttesystemer.

De vanligste kontorstøttesystemene er:

- tekstbehandlingsprogram
- regneark
- presentasjonsprogram
- database
- program for prosjektstyring
- bildebehandlingsprogram og tegneverktøy
- e-post og planleggingsverktøy

Et mye brukt presentasjonsprogram er PowerPoint. Her fra tittellysbildet i PowerPoint 2007.
Opphavsmann: Microsoft

Tekstbehandling, regneark og presentasjon
Tekstbehandlingsprogram, regneark og presentasjonsprogram regnes som de tre viktigste kontorstøttesystemene, og så å si alle virksomheter bruker disse.

Databaser
Databaser er en svært variert gruppe av programmer. For eksempel er alle administrative systemer som regnskap, fakturering, lønn og lagersystemer basert på databaser. Det samme gjelder de aller fleste nettbutikkløsninger og bestillingssystemer på Internett.

Men når vi snakker om databaser som kontorstøttesystem, mener vi vanligvis enklere register som kunderegister, medlemsregister og lignende. Kjente programmer er Microsoft Access, SuperOffice og lignende CRM-løsninger. CRM er forkortelse for Customer Relationship Management, og CRM-programvare brukes til oppfølging av kunder og i markedsføringssammenheng.

Prosjektstyring

Programmer for prosjektstyring brukes for å holde orden på mål, milepæler, tidsforbruk, ressurser og kostnader i prosjekter. Typisk vil en prosjektleder bruke et prosjektstyringsprogram til planlegging, oppfølging og kontroll av et prosjekt. Videre har alle prosjektdeltakere tilgang til programmet, slik at de kan oppdatere informasjon fortløpende og følge med. Det finnes hundrevis av ulike programmer for prosjektstyring, og mange av dem er spesialisert for bestemte typer prosjekter og bransjer eller en bestemt prosjektmetodikk. De aller fleste prosjektstyringsverktøy er blitt nettbaserte, slik at prosjektdeltakerne har tilgang til informasjonen uavhengig av maskinplattform og hvor de befinner seg. Et eksempel på et nettbasert prosjektstyringsverktøy er Projectplace.

Større prosjekter med mange deltakere krever gode prosjekstyringsverktøy
Fotograf: Corbis

Bildebehandling og tegneverktøy

Bildebehandling er etter hvert blitt en vanlig kontoroppgave i mange virksomheter. Bildebehandlingsprogrammer og tegneverktøy som Adobe PhotoShop, Elements, Illustrator, PaintShop Pro og tilsvarende kan derfor også regnes som kontorstøtteprogrammer. Her har det også dukket opp mange nettbaserte alternativer.

E-post og planleggingsverktøy

E-post er en viktig kommunikasjonsform i de fleste virksomheter. I tillegg har de fleste behov for funksjoner som møteplanlegging, kalendere og kontaktlister. Microsoft Outlook er det meste brukte programmet, men Googles Gmail og kalender er også populær.

Det finnes en rekke andre programtyper som også kan kalles for kontorstøtteprogrammer. Noen eksempler er programmer for å lage tankekart, dele notater eller for å lage brosjyrer og publikasjoner.

Det er også viktig å merke seg at stadig flere kontorstøtteprogrammer blir internettbaserte. Verktøy for prosjektstyring og programmer for deling av notater finnes nesten utelukkende som nettbaserte systemer, og det finnes nettløsninger for alle typer kontorstøtteprogrammer.

Programvare for e-post er en selvsagt del av kontorstøtteprogrammene i enhver bedrift.
Fotograf: NKI Forlaget

Kontorstøttesystemer er en samlebetegnelse på programvare for vanlige kontoroppgaver.

Betingelser for effektivisering

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Betingelser for effektivisering (120242)

Hensikten med å bruke programmer for kontorstøtte er å effektivisere, forenkle eller automatisere vanlige arbeidsoppgaver.

Brevflettingsfunksjonen i tekstbehandlingsprogrammer er et eksempel på en funksjon som både automatiserer, effektiviserer og forenkler en oppgave som tidligere kunne ta svært lang tid. Men en oppgave blir ikke alltid enklere eller raskere ved å bruke et dataprogram.

Eksempel: arkivsystem

Se for deg en virksomhet som har et arkivskap hvor alle kontrakter er arkivert alfabetisk. Dette synes vi er tungvint og gammeldags, så vi bestemmer oss for å begynne å skanne alle kontraktene og lagre dem i et dokumentsystem isteden. Ved å bruke programvare for karaktergjenkjenning blir innholdet i dokumentene søkbare, og de kan enkelt hentes fram på skjermen.

Vi installerer systemet og begynner å skanne inn og registrere alle kontraktene som ligger i arkivskapet. Denne jobben tar flere uker. Men når alt endelig er på plass, oppdager vi at virksomheten allikevel må ta vare på papirkopier av alle kontrakter av hensyn til signaturene. Videre er det ikke noe stort behov for å kunne søke på teksten i de enkelte kontraktene, og de som har behov for å se hva som står i en kontrakt, foretrekker å finne fram originalen fra arkivskapet.

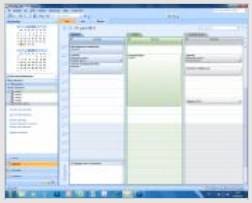
Resultatet er at vi har laget et system som verken forenkler arbeidet eller gir noen effektivitetsgevinst. Tvert imot tar arkivering nå lengre tid fordi alle nye kontrakter også skal skannes og legges inn i dokumentsystemet i tillegg til å arkiveres i arkivskapet. Vi har også hatt kostnader til programvare og utstyr, til å skanne alle de gamle kontraktene, og antakelig til brukeropplæring. Det å ta i bruk kontorstøttesystemer er altså i seg selv ikke noen garanti for at arbeidet blir mer effektivt.

Mengden papir i et arkiv kan bli enorm. Da kan det lønne seg å skanne dokumentene og bygge opp et digitalt arkiv i stedet, eller …?
Fotograf: Espen Bratlie

Eksempel: delt kalenderfunksjon

En del kontorstøttesystemer fungerer bare når alle i virksomheten tar det i bruk. Et eksempel er en delt kalenderfunksjon som gir mulighet til å registrere når man er opptatt, har ferie eller er på reise, slik at alle i virksomheten enkelt kan sjekke når andre er tilgjengelige. Et slikt system kan være svært effektiviserende for planlegging av møter og lignende. Men hvis ikke alle tar det i bruk og oppdaterer kalenderen sin regelmessig, kan ikke andre stole på den informasjonen som er lagt inn, og systemet blir mer til bry enn til hjelp.

For å sikre at vi oppnår den gevinsten vi ønsker ved å innføre et kontorstøttesystem, må vi først undersøke om det er mulig å løse oppgaven ved hjelp av et kontorstøttesystem, og om systemet faktisk vil gjøre arbeidet enklere eller mer effektivt.



For at delt kalenderfunksjon skal fungere godt, bør alle i bedriften registrere sine møter der.
Opphavsmann: NKI Forlaget

Deretter må vi finne ut hva det vil kreve av endringer i arbeidsrutiner for at systemet skal fungere som planlagt.

I eksemplet med arkivsystemet var det ikke mulig å løse oppgaven med et kontorstøttesystem fordi papirkopiene av kontraktene uansett måtte arkiveres manuelt. I eksemplet med delt kalenderfunksjon er det manglende rutiner som skaper problemer.

Vi oppnår vanligvis den største effektiviseringen for oppgaver som gjøres regelmessig eller skal gjøres mange ganger. For eksempel kan bruk av regneark være svært effektiviserende ved arbeid med budsjetter, hvor tallene ofte skal endres mange ganger før man er ferdig. Men for en utregning som bare skal gjøres én gang, kan det være like effektivt å bruke en kalkulator og papir og penn.

En oppgave blir ikke alltid enklere eller raskere ved å bruke et dataprogram.

Kontorstøttesystemer og nye rutiner

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kontorstøttesystemer og nye rutiner (120229)

Når en virksomhet tar i bruk et program for å gjøre en oppgave som tidligere er gjort manuelt, krever det ofte at eksisterende rutiner endres og tilpasses det nye systemet.

Siden de fleste kontorstøttesystemer tas i bruk for å effektivisere oppgaver som gjøres regelmessig, finnes det vanligvis allerede etablerte rutiner for hvordan oppgavene skal gjøres. For å få fullt utbytte av et nytt system må disse rutinene ofte endres og tilpasses systemet.

Når en virksomhet skal ta i bruk et nytt kontorstøttesystem, forventer de at oppgavene som systemet skal løse, tar kortere tid og blir enklere. Det stemmer som regel også, men gevinsten er ikke alltid umiddelbar.

La oss tenke oss en ansatt som har en arbeidsoppgave som gjøres manuelt. Denne bruker han vanligvis ca. fem timer på hver dag. De resterende tre timene av arbeidsdagen har han andre oppgaver som han også må gjøre.

Virksomheten bestemmer seg for å ta i bruk et kontorstøttesystem som vil redusere tida det tar å gjøre arbeidsoppgaven, til tre timer. Det vil frigjøre to timer som den ansatte kan bruke til andre oppgaver.

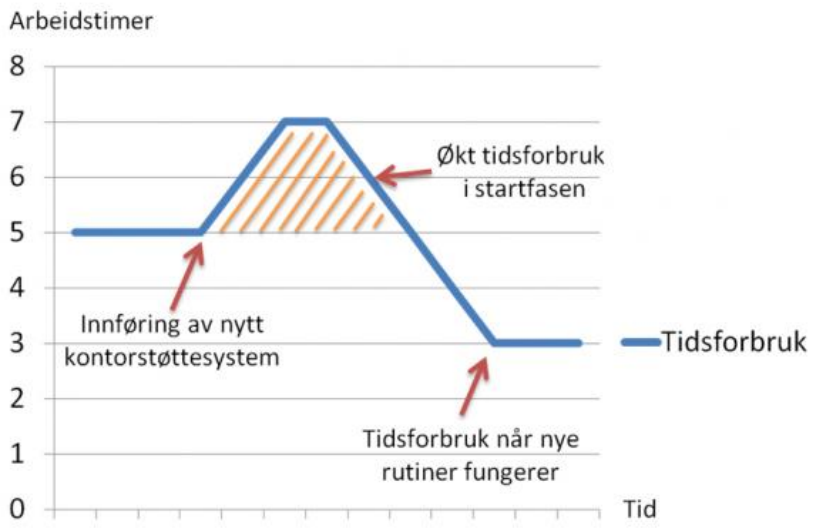
Målet med nye kontorstøttesystemer er som regel å effektivisere, det kan imidlertid ta tid før man når det målet.

Systemet blir installert og den ansatte får opplæring. Når systemet tas i bruk, får den ansatte samtidig en del nye arbeidsoppgaver for å fylle opp de to timene som nå blir ledige.

Men istedenfor å bruke to timer mindre, viser det seg at oppgaven nå tar to timer lengre tid enn tidligere. Dette skaper en uholdbar arbeidssituasjon for den ansatte, som må bruke sju timer på den oppgaven som tidligere tok fem timer. Han må fortsatt gjøre de andre oppgavene som tar tre timer, og i tillegg har han fått nye oppgaver som også tar to timer. Det som tidligere var en åtte timers arbeidsdag, er plutselig blitt til tolv timer.

Det tar naturlig nok ikke lang tid før den ansatte protesterer og forlanger å få gå tilbake til den gamle måten å arbeide på.

Dette er dessverre et altfor vanlig scenario fordi man glemmer at når en kjent oppgave skal gjøres på en ny måte, tar det tid å innarbeide nye rutiner. Dermed tar kjente arbeidsoppgaver i begynnelsen ofte lengre tid enn tidligere, inntil man blir fortrolig med en ny måte å jobbe på. Dette er vist i illustrasjonen under.



Tidsbruk i forbindelse med innføring av nye kontorstøttesystemer.

Effektivitetsgevinsten kommer etter hvert, men i startfasten kan det være frustrerende å oppleve at arbeidsdagen ikke lenger strekker til.

Ledelsen må derfor være oppmerksomme på at ansatte som skal ta i bruk et nytt system, i begynnelsen kanskje ikke rekker like mange oppgaver som før systemet ble innført. Dette må ledelsen legge til rette for.

God opplæring før systemet tas i bruk gjør at perioden før gevinsten oppnås, blir kortere, men nye rutiner må gjerne tilpasses etter at systemet er tatt i bruk. Opplæring kan derfor ikke alltid løse hele problemet.

For å få fullt utbytte av et nytt system må eksisterende rutiner ofte endres og tilpasses systemet.

Opplæring

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Opplæring (120235)

Som for alle nye systemer må brukerne få opplæring før et nytt kontorstøttesystem tas i bruk.

Gjennomføring av kurs i kontorstøttesystemer er grundig behandlet i kompetansemål 6 i faget Bruker og driftsstøtte.

- Planlegging og gjennomføring av enkle kurs

Kostnader

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Kostnader (120230)

Når du som IKT-medarbeider skal gi råd om kontorstøttesystemer, må du også si noe om kostnadene som innføring av et nytt system fører med seg.

For kontorstøttesystemer og andre standard programpakker må virksomheten betale for programvarelisenser.

Virksomheten ønsker ikke å betale for flere lisenser enn den trenger. Samtidig må vi være sikre på at vi ikke bruker programmer uten å betale for dem – det er i praksis det samme som å bruke piratkopiert programvare.

Det er viktig å passe på at bedriften har riktig antall og type lisenser.

Programvarelisenser kan være knyttet til

- antall brukere
- antall samtidige brukere
- antall maskiner programmet er installert på

For en lisens som er knyttet til antall brukere, betaler vi for hver person som bruker programmet, men hver person kan godt ha programmet installert på flere maskiner.

For en lisens som er knyttet til antallet samtidige brukere, betaler vi bare for så mange som skal kunne bruke programmet samtidig. Slike lisenser benyttes blant annet for mange serverbaserte eller internettbaserte applikasjoner. Hvis vi for eksempel har lisens for 20 samtidige brukere av et program, og alle lisensene er i bruk, vil en ny bruker ikke få tilgang til programmet før en annen logger seg ut.

For en lisens som er knyttet til antall maskiner programmet er installert på, betaler vi for antallet installasjoner uavhengig av hvor mange som bruker programmet. Du kan også komme over programmer som bruker en kombinasjon av ulike lisenstyper.

Det er også viktig å sjekke om programlisensen er en engangskostnad, eller om den gjelder for et begrenset tidsrom slik at den må fornyes regelmessig.

Vurdering av andre kostnader som et nytt system fører med seg, er behandlet i kompetansemålet «Dokumentere IKT-bruk og vurdere kostnads- og nytteverdien av et IKT-system».

Kostnader

Totale eierkostnader

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Totale eierkostnader (110717)

Kostnadene ved å investere i, drive og vedlikeholde IKT-systemer blir nesten alltid undervurdert, og totalsummen er ofte langt større enn prisen på bare maskin- eller programvaren. Derfor er det viktig å få fram de totale eierkostnadene ved IKT-systemer.

I IKT-bransjen brukes gjerne en analysemodell som kalles TCO (Total Cost of Ownership eller «totale eierkostnader» på norsk) for å beregne de totale kostnadene ved å investere i, drive og vedlikeholde IKT-systemer.

TCO-analysen forsøker å kartlegge alle kostnader forbundet med IKT-systemene.
Fotograf: Gorm Kallestad

TCO-analyser ble opprinnelig utviklet av analysefirmaet Gartner Group, men i dag finnes det en rekke ulike varianter og beregningsmetoder. Felles for alle TCO-analysene er at de forsøker å beregne de totale kostnadene en virksomhet blir belastet med når de velger å ta i bruk ny teknologi.

Siden TCO også inkluderer de indirekte kostnadene ved IKT-investeringer, får vi med kostnader som normalt ikke er synlige som IKT-kostnader i budsjetter og regnskaper. En annen viktig egenskap ved TCO-analyser er at de tar hensyn til kostnader som løper gjennom hele investeringens levetid, og ikke bare ser på hva den koster på investeringstidspunktet.

Kostnader som kan være med i en analyse av de totale eierkostnadene, inkluderer

- kapitalkostnader
- anskaffelseskostnader
- installasjonskostnader
- implementeringskostnader
- opplæringskostnader
- kostnader til drift og brukerstøtte
- servicekostnader
- merkostnader

Kapitalkostnader

Når en virksomhet investerer i et nytt IKT-system, må det naturlig nok betales. Hvis investeringen fører til at vi må låne penger, må vi ta med **rentekostnadene** for lånet i TCO-analysen, fordi dette er en kostnad som skyldes investeringen.

Låner bedriften penger i banken for å kunne investere i nytt IKT-utstyr, må rentene regnes med som en del av totalkostnadene.
Fotograf: Bob Strong

Men selv om vi har pengene fra før og ikke trenger å låne, er det fortsatt et alternativ å la pengene bli stående i banken eller plassere dem i noe annet som gir **avkastning**. Når vi velger å bruke pengene på en IKT-investering, mister vi de mulige renteinntektene vi kunne fått. I en TCO-analyse bør vi derfor ta med kapitalkostnadene – enten vi har pengene fra før eller må låne dem.

Anskaffelseskostnader

Anskaffelseskostnadene er den prisen vi betaler for utstyret eller programvaren ved anskaffelse. Dette er de enkleste kostnadene å få oversikt over, men vær oppmerksom på at mange programsystemer også har en **lisensavgift** som skal betales årlig. Dette må vi selvsagt ta hensyn til når vi skal beregne de totale kostnadene for hele investeringens levetid.

Installasjonskostnader

Installasjonskostnader er kostnader knyttet til selve installasjonen av utstyr og programvare. Det kan for eksempel være honorarer til leverandøren av systemet hvis han står for installasjonen, eller kostnader til trekking av kabler, ombygging av datarom eller lignende.

I tillegg til selve installasjonskostnadene kommer også eventuelle kostnader til testing av systemet før selve installasjonen gjennomføres.

Implementeringskostnader

Det kan være kostnader forbundet med å tilpasse ny teknologi til eksisterende løsninger eller rutiner. Tilpassing til eksisterende løsninger kan for eksempel være kommunikasjon med annet utstyr, datautveksling mellom ulike programmer og lignende. Slike kostnader kan være vanskelige å identifisere på forhånd.

Enda vanskeligere kan det være å beregne eventuelle kostnader som kommer fordi eksisterende **rutiner** i bedriften må legges om på grunn av det nye IKT-systemet. Dette skal ikke undervurderes, siden nye IKT-løsninger ofte medfører at kjente arbeidsoppgaver må gjøres på andre måter enn de ansatte er vant til. I en overgangsperiode kan det blant annet føre til at det tar lengre tid å utføre oppgavene.

Endringer av IKT-løsninger kan også få konsekvenser langt utover – og på helt andre områder enn – de oppgavene som løsningen i utgangspunktet var beregnet for. Innføringen av et nytt dokumentsystem kan for eksempel bety at man må legge om rutinene for hvordan dokumenter arkiveres, mens et nytt regnskapssystem kan føre til at man også trenger nye systemer for å registrere salg. Slike konsekvenser kan være uoversiktlige og derfor vanskelige å beregne.

Med **avkastning** mener vi for eksempel det utbyttet vi får av et arbeid, eller den gevinsten vi får i form av renter på et bankinnskudd.

Med avkastning mener vi for eksempel det utbyttet vi får av et arbeid, eller den gevinsten vi får i form av renter på et bankinnskudd.
Fotograf: Jan Djenner

Omlegging til nye arbeidsrutiner som følge av nye IKT-systemer kan ofte ta lang tid.
Fotograf: Henrik Sørensen

Opplæringskostnader

Nye IKT-systemer krever alltid opplæring. Ofte er dette synlig i form av kurs og læremateriell som har en fastsatt pris, men det er flere kostnader knyttet til opplæring. Selv når det ikke er behov for noe kurs eller spesiell opplæring, vil brukerne bestandig bruke en del tid på å gjøre seg kjent med det nye systemet, utforske nye funksjoner og prøve seg fram. Dette er også en form for læring, og tida som går med til å «fikle med systemet», må derfor regnes med i kostnadene.

Vi bør også ta med at kurs og opplæring fører til tapt arbeidstid for dem som deltar. Til sist må vi huske at det ikke bare er brukerne som trenger opplæring, men også de som skal drifte systemet og stå for brukerstøtten.

Det er viktig å sette av tid og penger til opplæring for de ansatte når man går over til nye IKT-systemer.
Fotograf: C. Devan

Kostnader til drift og brukerstøtte

Kostnadene til brukerstøtte i TCO-analysen inkluderer alle kostnader til brukerstøtte når systemet er i drift, for eksempel ekstern brukerstøtte eller kundehjelp. I virksomheter som har fast ansatte IKT-servicemedarbeidere, tar man i noen analyser også med en del av lønnskostnadene til disse avhengig av hvor mye tid man mener vil gå med til å besvare spørsmål, løse problemer og hjelpe brukere med det nye systemet.

Servicekostnader

Servicekostnader er kostnader til teknisk service og serviceavtaler. Dette er ofte eksterne kostnader som timepris for en servicetekniker eller en årlig serviceavtale til et fast beløp.

Merkostnader

Investering i et nytt IKT-system kan føre til at vi pådrar oss andre kostnader som en konsekvens av investeringen. Et nytt program kan for eksempel kreve raskere og kraftigere datamaskiner eller større skjermer. Nytt maskinutstyr kan gi dyrere forsikring. Et system for online-registrering av bestillinger ute hos kunde ved hjelp av bærbar pc og mobiltelefon gir høyere mobiltelefonregninger og så videre. De siste årene har man også begynt å inkludere eventuelle kostnader som følge av behovet for økt sikkerhet.

Når vi beregner TCO, er de største kostnadene ofte knyttet til lønnskostnader for de ansatte. Det kan være litt vanskelig å se hvorfor lønn til fast ansatte skal regnes med, siden virksomheten jo må betale den samme lønnen enten den investerer i nytt utstyr eller ikke. Grunnen er at man antar at den tida som blir benyttet til installasjon, brukarstøtte, opplæring og så videre, ellers ville vært benyttet til annet arbeid.

Enkelte programmer krever større og bedre skjermer – eller flere skjermer – for optimal utnyttelse. Dette kan bidra til å øke kostnadene ved implementering av nye IKT-systemer.
Fotograf: Ken Seet

Kostnadene til investeringer, drift og vedlikehold av IKT-systemer blir nesten alltid undervurdert.

Når du skal arbeide med å kartlegge IKT-kostnader, kan det være lurt å bruke et **regneark**. Her kan du repetere det du lærte om regneark på Vg1.

Totale eierfordeler

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Totale eierfordeler (110749)

Vi kan ikke ta en avgjørelse om en investering bare ut fra hva investeringen koster. Når vi beregner TCO for en IKT-løsning, må vi samtidig beregne hvilke fordeler virksomheten oppnår ved å investere i løsningen. Dette kalles for TBO (Total Benefits of Ownership, eller «totale eierfordeler» på norsk).

Selv om TCO-analyser kan få det til å se ut som om ingen IKT-investeringer vil være lønnsomme, er det viktig å være klar over at de totale eierkostnadene ofte også er det viktigste argumentet for å investere i nytt utstyr. Siden de totale IKT-kostnadene bare i liten grad er knyttet til prisen på utstyret (anskaffelseskostnadene), vil en investering i nytt utstyr fort kunne vise seg bli langt mer lønnsom enn å beholde en eksisterende løsning hvis den nye løsningen erstatter høyere TCO-kostnader for de løsningene man allerede har.

Fordeler som kan være med i en analyse av de totale eierfordelene, er

- effektiviseringsfordeler
- servicefordeler
- konkurransefordeler
- styringsfordeler
- kostnadsfordeler
- sikkerhetsfordeler

Effektiviseringsfordeler

Effektiviseringsfordeler kan hentes ut på mange områder og måter, men felles for dem alle er at de gir innsparinger ved at det nye systemet gjør en oppgave enten enklere eller raskere, slik at man trenger færre personer eller mindre tid for å utføre den. Dette reduserer virksomhetens lønnskostnader, og for de fleste virksomheter er dette den desidert største utgiftsposten i regnskapet.

For en virksomhet som vurderer å oppgradere eller skifte ut et eksisterende system, vil en reduksjon av TCO-kostnader for det eksisterende systemet være en effektiviseringsgevinst. Mange systemoppgraderinger gjøres nettopp av denne grunn.

Servicefordeler/konkurransefordeler

Innføring av nye IKT-systemer, for eksempel på et større lager, kan bidra til å effektivisere arbeidet, slik at man får minimalt med manuelt papirarbeid.
Fotograf: Corbis

Ved Telemark sentralsykehus har de lenge benyttet IKT-teknologi for å formidle viktig informasjon. I dette tilfellet deler røntgenlegene nødvendige bilder seg imellom. Du kjenner kanskje til tilfeller i helsesektoren der IKT ikke blir utnyttet i den grad den burde?
Fotograf: Jan Tomas Espedal

Nye IKT-systemer blir ofte innført for å øke virksomhetens servicegrad overfor kunder eller gi en virksomhet et konkurransefortrinn framfor sine konkurrenter. En bedrift henter gjerne ut en slik fordel som høyere salg, mens en organisasjon som ikke har et økonomisk mål, kan hente ut fordelen ved at den yter bedre eller raskere service og dermed får flere og mer fornøyde kunder. En servicefordel for et sykehus vil for eksempel være at de kan behandle flere pasienter.

Servicefordeler kan hentes ut på mange måter. For eksempel vil et system med bedre driftssikkerhet ofte kunne gi både en servicefordel og en effektiviseringsfordel.

Styringsfordeler

Virksomheten henter ut styringsfordeler ved at den får bedre kontroll med den delen av virksomheten som det nye systemet håndterer. Ved at virksomheten for eksempel får tilgang til bedre informasjon på et tidligere tidspunkt, reduseres faren for gale beslutninger eller at beslutningene blir tatt for sent. Styringsfordeler er også et viktig middel for å gjøre en virksomhet mer fleksibel, slik at den kan omstille seg raskere til endringer i marked eller samfunn.

Kostnadsfordeler

Et IKT-system kan også bidra til å redusere kostnader ved at den overflødiggjør utstyr eller rutiner som påfører virksomheten ekstra kostnader. Sammenlignet med effektiviseringsfordeler som gjør en oppgave enklere eller raskere, vil en kostnadsfordel innebære at en oppgave kan gjøres rimeligere selv om den fortsatt tar like lang tid og krever like mange mennesker.

Sikkerhetsfordeler

Nye IKT-systemer har som regel et betydelig høyere sikkerhetsnivå enn forgjengerne. Dette kan i seg selv ses på som en fordel, og det blir ofte benyttet som et argument for en investering.

Sikkerhetsfordeler gir ikke noen direkte gevinst i form av inntekter, reduserte kostnader, bedre service eller lignende. Fordelen ligger først og fremst i at man har redusert risikoen for at det skal skje noe som vil påføre virksomheten høye kostnader eller ha andre alvorlige konsekvenser.

Det er viktig å ha gode data og nøyaktig informasjon om driften slik at bedriften kan ta riktige avgjørelser om hva den skal gjøre i framtida. IKT-verktøy kan gi virksomheten tilgang til disse dataene. Her orienterer konsernsjef Svein Richard Brandtzæg om Norsk Hydros resultater.
Fotograf: Knut Falch

Gamle IKT-systemer og andre administrative systemer kan ofte være svært dyre å beholde fordi de krever spesialkompetanse for drift og vedlikehold – en kompetanse som er gått ut på dato ellers i samfunnet. Bruken av den gamle hullkort-teknologien kan kanskje være et eksempel på dette (bildet er fra 1953).
Fotograf: Aktuell

Når vi beregner totale eierkostnader, må vi også beregne totale eierfordeler.

Innsparinger gir ikke alltid lavere kostnader

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innsparinger gir ikke alltid lavere kostnader (110755)

Selv om det alltid er et mål å redusere kostnader, må vi også være oppmerksomme på at en innsparing på ett område kan føre til økte kostnader på et annet.

I de fleste virksomheter er IKT først og fremst en servicefunksjon som skal hjelpe bedriften eller organisasjonen med å oppnå sine mål. Selv om IKT-systemene ofte er svært viktige verktøy for driften, er det vesentlig for alle typer virksomheter å holde kostnadene nede for servicefunksjoner, og dette gjelder selvsagt også for IKT.

Mange IKT-kostnader er lette å se i regnskapet og derfor et enkelt mål når det er behov for innsparinger. Men en fare ved å fokusere for mye på IKT-kostnader i denne sammenhengen er at man kan overdrive innsparingene.

Hvis innsparinger fører til at nedetid, responstid, servicetid eller antall feil øker, fører det igjen til at flere ansatte blir sittende lenger uvirksomme, eller må bruke mer tid på å forsøke å løse IKT-problemer selv. Det kan fort bli svært kostbart uten at det umiddelbart vises i regnskapet.

Selv om en god IKT-servicemedarbeider er kostnadsbevisst og vil forsøke å redusere kostnadene der det er mulig, kan han eller hun ende i en situasjon hvor det er like viktig å argumentere for at bedriften må bruke *mer* penger på IKT, eller i det minste ikke redusere budsjettene ytterligere.

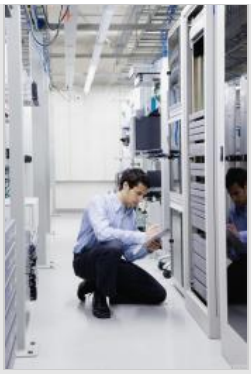
Siden konsekvensene ikke alltid er like åpenbare for dem som er ansvarlige for økonomistyring i virksomheten, er det viktig å kunne dokumentere hvilke effekter en reduksjon vil ha.

Mangelfull opplæring kan gi økte kostnader

Stengingen av Altinn-portalen våren 2012 som følge av stor pågang fra folk som ønsket å se selvangivelsen sin, fikk bred dekning i media. Feil på IKT-systemene – enten de skyldes et ønske om innsparing eller andre ting – kan koste bedriften dyrt både, både når det gjelder penger og negativ omtale. Fotograf: Erik Johansen

Dersom brukerne ikke har fått opplæring i den nye programvaren, kan dette medføre store kostnader i form av brukerstøtte og oppfølging senere. Fotograf: Royalty-Free

Et eksempel på en innsparing som kan gi økte kostnader, er opplæring. Mangelfull opplæring av brukerne fører ofte til at kostnadene til brukerstøtte stiger. Jo mindre opplæring brukerne har fått, jo oftere vil de ha behov for hjelp i ettertid. Det samme gjelder mangelfull opplæring av IKT-servicemedarbeidere fordi de da bruker lengre tid på å finne løsningen på problemer som kanskje er elementære.



Når bedriften har god dokumentasjon på tidligere oppståtte feil og løsninger, kan IKT-servicemedarbeideren raskt løse problemer som oppstår.
Fotograf: Corbis

En fare ved å fokusere for mye på IKT-kostnader er at man overdriver innsparingene.

Mangelfull dokumentasjon kan gi økte kostnader

Et annet eksempel på en innsparing som kan gi økte kostnader, er dokumentasjon. Selv om de ressursene som brukes til å dokumentere IKT-systemer, problemløsing og rutiner, ikke alltid gir noen umiddelbar gevinst for virksomheten, vil god dokumentasjon kunne ha stor betydning over tid.

Ved å sørge for man har oversiktlig og god dokumentasjon over IKT-utstyr, rutiner og eventuelle feil og problemer som oppstår, kan virksomheten hente ut en betydelig gevinst fordi det er lett å finne fram løsningen på tidligere problemer, og det er enkelt å orientere seg om konfigurasjoner eller annet som er av betydning for feilsøking, vedlikehold eller oppgradering av utstyr og programvare.

Mangelfull forebyggende brukerstøtte kan gi økte kostnader

Et siste eksempel er innsparinger når det gjelder forebyggende brukerstøtte. Det er vanligvis rimeligere å forebygge problemer enn å vente til noe går galt.

Behovskartlegging

Innledning til analyse av brukerstøtte

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Innledning til analyse av brukerstøtte (123611)

Virksomheter investerer i datasystemer for å bli mer effektive, og mange virksomheter er så avhengige av datasystemene sine at de ansatte i praksis blir sittende uten å kunne gjøre noe hvis de ikke fungerer som de skal.

Datasystemer som ikke fungerer, kan medføre store kostnader i form av tapt arbeidstid, tapte salg, forsinkelser, irriterte kunder og så videre. Det er derfor viktig at brukere får hjelp når de trenger det, og at problemer løses raskt.

Virksomheter som har en ineffektiv brukerstøtte, eller som forsøker å spare penger på brukerstøtte, ender ofte opp med å tape mer enn de sparer. Å organisere en effektiv og godt fungerende brukerstøtte er derfor en god investering for de fleste virksomheter.

Internt velger noen virksomheter å ha én eller flere ansatte IKT-medarbeidere som jobber med brukerstøtte, og som brukerne kan kontakte når de har problemer. En annen mulighet er å organisere brukerstøtten som en egen hjelpetjeneste (helpdesk), eller å sette bort brukerstøtten til et firma som har spesialisert seg på dette (outsourcing). Virksomheter som leverer IKT-løsninger til andre, må i tillegg ha en ekstern brukerstøtte for sine kunder.

Siden effektiv brukerstøtte kan være avgjørende for virksomheten, må vi hele tida sørge for at den fungerer best mulig. Et ledd i dette er regelmessig å analysere de henvendelsene som kommer til brukerstøtte for å se om det er behov for endringer, opplæring eller bedre brukerveiledninger.

Forutsetningen for å kunne analysere henvendelser til brukerstøtte er at alle henvendelser og oppfølgingen av dem registreres systematisk. Det gjelder også når virksomheten har overlatt brukerstøtten til et eksternt selskap.

Problemer med IKT-systemer som ikke virker, kan forårsake store frustrasjoner og vansker for bedriftens ansatte.
Fotograf: Mike Schröder

Statistikk og grafiske framstillinger kan brukes for å analysere brukerhenvendelser til en helpdesk.
Fotograf: Anders Wiklund

Ved å registrere alle henvendelser og oppfølgingen blir det mulig å ta ut rapporter og statistikk som kan analyseres for å finne ut hvordan vi kan øke brukernes tilfredshet og effektivisere brukerstøtten.

Alle forespørsler må registreres. Selv om problemet kan løses med en gang, er det viktig for senere analyser at også de sakene som ikke krever noen videre behandling, er registrert i systemet.

Videre må alle som er involvert i å løse en sak, registrere hva de gjør, slik at det blir mulig å gå tilbake og se hvor mye tid som går med til brukerstøtte.

Vi må også huske at brukerstøtte er en kostnad, og at det alltid er et mål i alle typer virksomheter å redusere kostnader. Når vi analyserer brukerstøtte, er det derfor også for å finne muligheter for å effektivisere på en slik måte at vi reduserer kostnadene uten at det går ut over brukerens tilfredshet og virksomhetens produktivitet.

Forutsetningen for å kunne analysere henvendelser til brukerstøtte er at alle henvendelser og oppfølgingen av dem registreres systematisk.

Analysere brukerstøtte

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Analysere brukerstøtte (123613)

Når vi skal analysere brukerstøtten, tar vi utgangspunkt i de henvendelsene som er registrert i en gitt tidsperiode, og tallfester dem.

Systemer for registrering av henvendelser til brukerstøtte, helpdeskprogramvare og lignende har gjerne innebygget rapport- og statistikkfunksjoner for analyseformål. Ofte kan tallene fra et slikt system også eksporteres til regneark for videre behandling.

Registrering av typer – og ikke bare antall – brukerhenvendelser kan danne grunnlaget for å utvikle brukerstøttefunksjonen i bedriften.
Fotograf: Corbis

Hvilke parameter vi skal undersøke, varierer fra virksomhet til virksomhet og er avhengig av hva som blir registrert i systemet. Tall som kan være aktuelle, er:

- hvor mange forespørsler kommer det per dag, uke eller måned
- hvordan belastningen fordeler seg per dag, uke eller måned
- hvilke typer forespørsler brukerstøtten får
- hvordan forespørslene fordeler seg på systemer og produkter
- hvor lang den gjennomsnittlig responstida er ved henvendelse til brukerstøtten
- hvor lang den gjennomsnittlige servicetida er fra brukeren henvender seg til problemet er løst
- hvilke typer problemer det tar lengst tid å løse
- hvor mange forespørsler løses
- hvor mange forespørsler som ikke kan løses

Hvor mange henvendelser brukerstøtte får, og hvordan de fordeler seg i løpet av en dag, uke og måned, kan fortelle oss om det er bestemte dager eller tider på døgnet da det er behov for høyere bemanning.

Et firma som leverer regnskapssystemer, kan for eksempel ha behov for å forsterke brukerstøtten i januar når de fleste kundene skal ta årsavslutning av regnskapet sitt.

Hvilke typer forespørsler brukerstøtte mottar, og hvilke systemer og produkter det er flest problemer med, kan fortelle oss om det er bestemte systemer eller problemer som går igjen. Det kan være et tegn på at det er behov for mer opplæring av brukere eller bedre brukerveiledninger.

Hvor lang responstida og servicetida er, forteller oss hvor effektiv brukerstøtten er. Ved å sammenligne tallene for flere perioder kan vi også se utviklingen over tid. Hvilke problemer det tar lengst tid å løse, kan fortelle oss noe om behovet for opplæring av IKT-medarbeidere som jobber med brukerstøtte.

Analyser av henvendelser til brukerstøtte kan også kombineres med brukerundersøkelser som vi så på i kompetansemålet «Gjennomføre en undersøkelse av brukertilfredsheten i en virksomhet og vurdere resultatet mot organiseringen av brukerstøtten og avtalt tjenestekvalitet».

For å kunne analysere henvendelser til brukerstøtte må vi først kunne tallfeste den informasjonen vi er interessert i.

Konsekvenser

Forfatter: Arne Jansen, NKI Forlaget, Amendor AS
Konsekvenser (123618)

Det har ingen hensikt å analysere brukerstøtte hvis det ikke får noen konsekvenser.

Det kan selvsagt tenkes at brukerstøtten og alle systemer fungerer helt som de skal, men det er nok mer sannsynlig at analysene viser at det finnes muligheter for forbedringer.

Ved å analysere henvendelser til brukerstøtte regelmessig er det også lettere å fange opp endringer som påvirker effektiviteten. Eksempel på endringer kan være oppdateringer av systemer, nye rutiner eller arbeidsprosesser i virksomheten, eller nye ansatte som ikke har fått opplæring.

Viktige spørsmål som virksomheten ønsker å få svar på, er:

- Hva er de faktiske kostnadene til brukerstøtte, og hvordan kan de reduseres?
- Hvordan kan kostnadene til brukerstøtte reduseres uten at det påvirker brukerens tilfredshet og produktivitet?
- Hvordan kan den generelle kvaliteten og effektiviteten for brukerstøtten forbedres?
- Hvor effektiv er vår brukerstøtte i forhold til konkurrenter eller andre sammenlignbare virksomheter?
- Hvor flink er brukerstøtte til å tilpasse seg endringer og oppdatere egne rutiner og systemer i takt med utviklingen?
- Hvilket behov har brukerne for opplæring?
- Kan deler av brukerstøtten automatiseres?

Kostnadene som går med til å opprettholde en god brukerstøttefunksjon, bør vurderes fortløpende.

Det er blitt vanlig å sette ut funksjonen IKT-støtte til land i Asia.
Fotograf: Amit Bhargava

Å automatisere brukerstøtten innebærer at vi innfører systemer som gjør at brukerne selv finner fram til løsningen på problemet sitt.

Det finnes flere ulike løsninger for automatisert hjelp, men de fleste er bygget opp rundt et system hvor maskinen spør brukeren en serie spørsmål om hva problemet består i, og deretter foreslår ulike løsninger i form av steg-for-steg-beskrivelser.

En annen vurdering som de fleste virksomheter må gjøre regelmessig, er om brukerstøtte skal overlates til et firma som har spesialisert seg på dette (outsourcing), eller om det skal være en funksjon internt i virksomheten.

Selv om vi vanligvis hører mest om outsourcing, kan også det motsatte være aktuelt, altså at virksomheten bygger opp egen kompetanse og overtar brukerstøttefunksjonen fra et eksternt firma. Dette kalles for insourcing og kan være aktuelt i tilfeller hvor eksterne firma ikke klarer å levere tilfredsstillende brukerstøtte.

Virksomheten kan for eksempel ha systemer som er så spesialiserte at det ikke finnes andre firma som har tilstrekkelig kompetanse til å støtte dem, eller at eksterne firma mangler forståelse for hva virksomheten driver med, og hvilke behov de har. En annen årsak kan være hensynet til sikkerhet eller personvern.

Ved å analysere henvendelser til brukerstøtte regelmessig er det også lettere å fange opp endringer som påvirker effektiviteten.

Oppgaver

Eksamensoppgaver

Eksamensoppgave 1

Forfatter: Jan Frode Lindsø
Eksamensoppgave 1 (138967)

Denne tverrfaglige oppgaven tar for seg sentrale kompetansemål i alle programfagene. Tidsplan og organisering tilsvarer tverrfaglig eksamen på Vg2 og kan variere noe fra fylke til fylke.

Forberedelse eksamen

Du jobber som førsteårslærling i kommunen, og det lokale idrettslaget skal arrangere fotballcup. Lederen i idrettslaget ber kommunen om assistanse, og du får i oppdrag å bistå med IKT-relaterte oppgaver under arrangementet. Du skal også være med på å planlegge en hensiktsmessig infrastruktur for IKT-systemene til idrettslaget. Fotballcupen har 145 påmeldte deltakere, og administrasjonen i idrettslaget – som også utgjør arrangementskomiteen – består av fem personer. I tillegg skal fire frivillige trenere hjelpe til med organiseringen og med registrering av resultatene. Administrasjonen ønsker å ha stasjonære PC-er på kontorene sine, mens de frivillige, som skal være ute ved fotballbanen, bør ha hver sin bærbare PC eller andre hensiktsmessige enheter. For at arrangørene og trenerne skal få tilgang til resultathåndteringen, kreves det trådløst nett. Dette nettet skal også være tilgjengelig for deltakerne. På grunn av størrelsen på arrangementet er det viktig at nettet er tilstrekkelig sikret. Arrangørene vet at du har god erfaring i å bruke sosiale medier og andre kommunikasjonskanaler. De ønsker derfor at du er med og markedsfører arrangementet og kommer med konkrete forslag til metoder for å gjøre informasjon tilgjengelig.

Drift og vedlikehold

- Drift av domeneserver for idrettslaget
  - Idrettslaget trenger en domeneserver for brukerhåndtering.
- Forslag til infrastruktur for IKT-system
  - Idrettslaget ønsker en ny infrastruktur for IKT-systemet sitt. De ber om råd i forbindelse med planlegging og oppsett av nettverk med det idrettslaget trenger av IKT-løsninger.
- Innkjøp av datautstyr
  - Idrettslaget trenger nytt datautstyr, spesielt til fotballcupen. De trenger datamaskiner, nettverksløsninger, programvare og annet som er hensiktsmessig for driften.

Bruker- og driftsstøtte

- Lagring av deltakerinformasjon
  - Arrangørene skal lagre informasjon om deltakerne og trenger derfor en innføring i personvern og lagring av personopplysninger.
- Tekstbehandling og regneark
  - De frivillige og administrasjonen har bare grunnleggende kjennskap til bruk av tekstbehandling og regneark. De vet derfor lite om hvordan de kan ta i bruk disse verktøyene på en måte som er nyttig for dette arrangementet.
- Forslag til etiske retningslinjer
  - Arrangørene har tatt i bruk hashtag #fotballcupen. De ønsker at deltakerne skal kunne publisere sine egne bilder. Samtidig ønsker de å gå ut med noen etiske retningslinjer til deltakerne.
- Brukerstøtte til idrettslaget
  - For at din brukerstøtte til idrettslaget skal bli mer effektiv, setter du opp et helpdesk-system for å betjene henvendelsene du får. Her må du svare, prioritere og henvise forespørslene på en hensiktsmessig måte.

Virksomhetsstøtte

- Anskaffelse av kontorstøttesystem
  - Administrasjonen må gå til anskaffelse av et kontorstøttesystem, og ønsker derfor å vite hva som er fordelene og ulempene med ulike systemer.
- Tilpassede løsninger
  - Arrangementet skal inkludere alle, også mennesker med nedsatt funksjonsevne. De ønsker derfor råd om hvordan de best mulig kan gjøre tilpasninger når det gjelder alt fra nettside til andre digitale hjelpemidler.
- Kartlegging av tilfredshet
  - Arrangørene ønsker å kartlegge tilfredsheten med arrangementet i etterkant. De ønsker derfor noen råd om hva de bør spørre om, og hvordan de bør analysere svarene. Resultatet skal brukes til å styrke neste års arrangement.

Oppgaver:

1. Administrasjonen sitter i et nettverk og har samlet felles dokumenter på en filserver. Opprett og del en mappe. Opprett deretter en bruker, og sett riktige rettigheter på mappen.
2. Det er mange utfordringer i forbindelse med barn og unge på nett, og arrangørene ønsker å vise seg som gode forbilder. Ta derfor for deg etiske problemstillinger knyttet til personvern under arrangementet. Skisser et forslag til en presentasjon for administrasjonen eller en veiledning til deltakerne.
3. Administrasjonen er usikker på hvilket kontorstøttesystem de bør ta i bruk. Ta for deg ulike kontorstøttesystemer og argumenter for de ulike valgene du har gjort. Ta hensyn til brukervennlighet, pris, funksjonalitet og tilgjengelighet.