IKT, informasjonssikkerhet og risiko

DRI1002
10.april 2007

Rune Jacobsen
ErgoGroup

Innhold

1. Kort om ErgoGroup og meg selv.
2. Utvikling i bruk av IKT og Internett.
3. Informasjonssikkerhet.
4. Risiko og risikovurdering
5. Risikovurderingsmetode

1.
Kort om ErgoGroup og meg selv

Kort om ErgoGroup og meg selv

- ErgoGroup er et av Nordens ledende IT-selskap, heleid av Posten Norge.
- Over 3000 ansatte, og med omsetning på over 5 milliarder kroner.
- Fire forretningsområder: Offentlig-løsninger, IKT-driftstjenester, SMB-løsninger og Forretningsløsninger.
- IKT-driftstjenester: Tele- og datakommunikasjonstjenester, serverdrift, outsourcing og applikasjonsforvaltning.

- Min rolle i ErgoGroup:
  Sikkerhetskontroller i Divisjon Infrastruktur. Skal hovedsakelig kontrollere etterlevelsen av divisjonens krav til informasjonssikkerhet.
- I tillegg jobber jeg med analyse av risiko samt rådgivning innenfor fagområdet.

2.
Utvikling i bruk av IKT og Internett

Utvikling i bruk av IKT

- I de siste 30 år, spesielt i de siste 10 årene, har det vært en voldsom økning i bruk av IKT.

- Effektive informasjonssystemer, som gir *korrekt informasjon* til *rett person* til *rett tid* slik at det blir mulig å ta *riktige beslutninger*, blir en stadig viktigere *konkurransefaktor*.

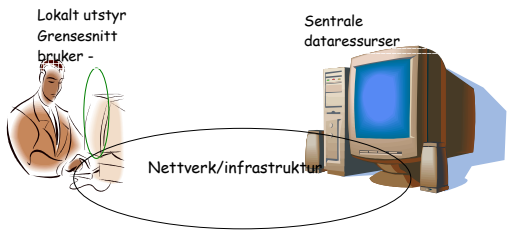
- I den samme perioden har antallet tilfeller av innbrudd i informasjonssystemer, fortrolig informasjon på avveie, manipulert informasjon og andre uønskede hendelser også blitt mangedoblet.

Nye kommunikasjonsløsninger

- Kommunikasjon internt i maskiner og mellom maskiner i lokale nettverk.
- Kommunikasjon mellom geografisk atskilte kontorer ved hjelp av dedikerte linjer (leide linjer).
- Kommunikasjon mellom geografisk atskilte kontorer ved hjelp av svitsjede lukkede nettverk, hvor trafikk fra forskjellige brukere ble logisk skilt.
- ”Alle-til-alle” kommunikasjon ved hjelp av Internett (TCP/IP):
  - Sammenknytning av geografisk atskilte kontorer
  - Økende behov for kommunikasjon med samarbeidspartnere og underleverandører
  - Hyppigere oppkjøp og sammenslåing av selskaper

Internett

- Internett protokollene (IPv4) ble opprinnelig laget med tanke på en kommunikasjon basert på åpenhet og fleksibilitet, og *ikke med tanke på sikkerhet*.
- Internett var opprinnelig et nett brukt av forsknings- og universitetsmiljøer.
- Nå skal ”alle” bruke Internett til ”alt”.
- De første sikkerhetshendelser på Internett ble allerede oppdaget på midten og mot slutten av 1980-tallet.
- Stadig nye trusler gir nærmest en kontinuerlig endring i trusselbildet.



Hvilke farer truer oss ?

- På lokalt utstyr:
  - Virus, ormer, hacking, informasjonskapler (cookies)
  - Dårlig brukergrensesnitt som skaper ’unødvendige’ feil
  - Menneskelige/organisatoriske feil
- I infrastrukturen
  - Avlytting, ødeleggelse/misbruk
  - Tyveri av identitet, falske nettsteder,
  - Trådløse nett innebærer spesielle sikkerhetsproblemer
- ”På sentrale ressurser
  - Virus, ormer, hacking,.tjenestenekting, kapasitetsproblemer, ..
  - Ikke tilfredsstillende kvalitet på informasjon

3. Informasjonssikkerhet

Sitat 1 – Salman Rushdie

- *Sikkerhet er kunsten å sørge for at visse ting ikke skjer.*

  En utakknemlig oppgave, for når slike ting ikke skjer, vil det alltid være noen som hevder at sikkerhetstiltakene var overdrevne og unødvendige.

Sitat 2 – Aristoteles

- *Det er sannsynlig at noe usannsynlig kommer til å skje.*

Informasjonssikkerhet

- *Informasjonssikkerhet er fravær av uønskede hendelser*

  Informasjonssikkerhet kan derfor sies å være en tilstand vi ønsker å befinne oss i.

Informasjonssikkerhet - Viktige begreper (1)

- ***Konfidensialitet***
  - Sikkerhet for at ***kun autoriserte brukere*** får tilgang til informasjonen.
- ***Integritet***
  - Sikkerhet for at informasjonen er ***fullstendig, nøyaktig og gyldig.***
- ***Tilgjengelighet***
  - Sikkerhet for at informasjonen ***er tilgjengelig for autoriserte brukere til rett tid***.

Informasjonssikkerhet - Viktige begreper (2)

- ***Autentisering***
  - Benyttes for å bevise at en bruker er den brukeren han eller hun utgir seg for å være.
- ***Autorisasjon***
  - Benyttes for å gi en bruker tilgang til kun den informasjonen eller til det informasjonssystemet han eller hun skal ha tilgang til.
- ***Ikke-benekting (nonrepudiation)***
  - Benyttes for at en bruker ikke senere skal kunne nekte for at det er han eller hun som har utført handlingen.

Informasjonssikkerhet - Definisjon

- Beskyttelse mot brudd på ***konfidensialitet***, ***integritet*** og ***tilgjengelighet*** for informasjonen i et informasjonssystem og for informasjonssystemet i seg selv.
- Sagt på en annet måte:
  Robuste og effektive informasjonssystemer, som gir ***korrekt informasjon*** til ***rette personer*** til ***rett tid***

Utfordringer

- Mange har ikke tilstrekkelig oversikt over:
  - *hvilken informasjon de eier og/eller behandler/har lagret*
  - *hvilken verdi informasjonen representerer for seg selv eller for andre*
  - *hvilken informasjon eller hvilke informasjonssystemer som er kritiske*
  - *hvilken konsekvens skade på eller tap av informasjon vil kunne utgjøre for seg selv eller andre*

Noen problemområder

- Ledelsen er ikke engasjert og tar ikke ansvar.
- Kostnader.
- Mangelfulle eller manglende rammeverk for sikkerhet (policy) og retningslinjer.
- Mangelfull teknologisk kompetanse.
- Manglende kunnskap om rettslige krav.
- Dårlige holdninger hos de ansatte.
- Fremvekst av ”usunne” bedriftskulturer.
- Konstant endring i trusselbildet.
- Illojale medarbeidere.

Suksessfaktorer

- Alle må ha et forhold til informasjonssikkerhet.
- Aktiv og engasjert ledelse.
- Kunnskap om krav til informasjonssikkerhet.
- Utarbeide policy og retningslinjer.
- Tilstrekkelig teknologi og kompetanse.
- Informasjon og opplæring av brukere.
- Sikkerhetsorganisasjon – Ansvar/myndighet.
- Riktige holdninger.
- Gradvis oppbygning av sikkerhetskultur.

Tilfredsstillende informasjonssikkerhet

- *For å kunne etablere og vedlikeholde et tilfredsstillende informasjonssikkerhetsnivå, kreves:*

  Et kontinuerlig og systematisk arbeid !!!

4. Risiko og risikovurdering

Risiko

- I Innst.S.nr.9 (2002-2003) står det:

  *Begrepet **risiko** benyttes til å karakterisere **hvor alvorlig en gitt type utfordring** mot vår sikkerhet **anses å være**.*

  ***Risiko** er et **produkt** av to faktorer: **Sannsynligheten** for at en sikkerhetsutfordring inntreffer og **konsekvensene** det vil få dersom den inntreffer.*

Styring av risiko mot krav til informasjonssikkerhet

- Kilder for krav til informasjonssikkerhet:
  - Rettslige regelverk - Lover og forskrifter
  - Sikkerhetsstandarder (”best practices”)
  - Virksomhetsspesifikke krav – Policy og retningslinjer
  - Avtaler
  - Personlige krav
  - Etiske normer

Risikovurdering – et systematisk hjelpemiddel for å styre risiko

- En risikovurdering skal identifisere sannsynligheten for og konsekvensen av en sikkerhetshendelse.
- En risikovurdering kan gjøres som en selvstendige vurderinger for relevante verdier i en virksomhet.
- Man må selv fastlegge kriterier for akseptabel risiko forbundet med den enkelte verdi.
- Dersom risikoen overstiger akseptabelt risikonivå, må tiltak innføres enten for å:
  - *Redusere sannsynligheten for at sikkerhetshendelsen inntreffer eller for å begrense skadeomfanget (konsekvensen) dersom sikkerhetshendelsen inntreffer.*

Konkret krav til gjennomføring av risikovurdering

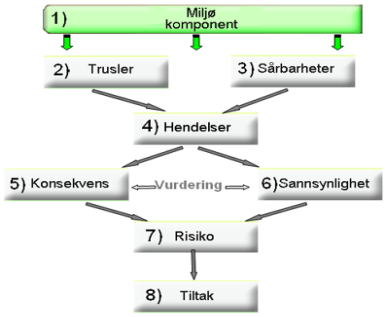
For de som etter lovens saklige virkeområde i pol. § 3 bokstav a utfører ”behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler”, er det et rettslig krav til ”tilfredsstillende informasjonssikkerhet” jf. pol. § 13. I henhold til pof. § 2-4 er det pålagt å gjennomføre en risikovurdering. Dette er et hjelpemiddel for å vurdere hva som skal til for at sikkerheten kan sies å være tilfredsstillende. Det som skal sikres er personopplysninger.

5. Risikovurderingsmetode

”Formkrav” til risikovurderingsmetode

- Etter Datatilsynet veiledning bør en risikovurdering i korte trekk inneholde disse elementene :
  - Kartlegging av personopplysninger
  - Fastsetting av kriterier for akseptabelt risikonivå
  - Kartlegging av trusler og sårbarheter
  - Kartlegging av uønskede hendelser
  - Vurdering av de uønskede hendelsenes konsekvens
  - Vurdering av sannsynlighet for at de uønskede hendelsene oppstår
  - Evaluering og beskrivelse av anslått risiko
  - Sammenlikning av akseptabel risiko og anslått risiko
  - Kartlegging av og eventuell implementering av relevante tiltak i de tilfeller der anslått risiko er høyere enn akseptabel risiko

Prinsipp for gjennomføring av en risikovurdering

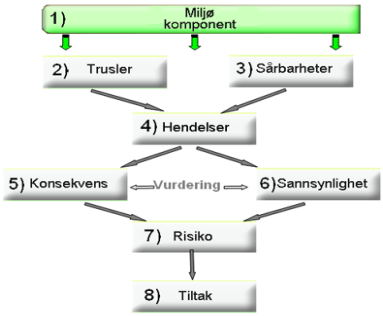


Hva er akseptabel risiko og hvordan bestemmer vi den?

- Vi må stille spørsmålet om hvor stor risiko vi er villige til å ta sett i forhold til ”våre” krav til informasjonssikkerhet:
  - Hvor mange ganger kan personopplysninger komme på avveie?
  - Hvor mange ganger kan vi miste familiebilder lagret på familiens PC?
  - Hvor mye kan vi tillate oss i refusjonskostnader for manglende leveranse av informasjonssikkerhet i henhold til avtale?
  - Hvor mye virksomhetssensitiv informasjon kan vi tillate oss å miste som følge av at ansatte mister eller blir frastjålet sine bærbare PC’er?
  - Hvor mange ganger kan vi bli ”hengt ut” i pressen for manglende informasjonssikkerhet før vi mener vårt omdømme blir alvorlig svekket.

Verdier – Hva må vi beskytte ?

Prinsipp for gjennomføring av en risikovurdering



Hva er en verdi

- Verdier er informasjon eller et informasjonssystem som kan påføres skade eller tapes som følge av en uønsket hendelse.
- Verdier må beskyttes.

Tre scenarioer

- ***Privatpersoner***
  – Hva ønsker vi å beskytte her
- ***Virksomhet i en spesifikk bransje***
  – Hva ønsker vi å beskytte her
- ***Tjenesteleverandør***
  – Hva ønsker vi å beskytte her

Verdier hos privatpersoner

- Familiebilder.
- Personlig informasjon.
- Kontoinformasjon.
- Materielt utstyr som for eksempel PC.

Verdier hos en virksomhet i en spesifikk bransje

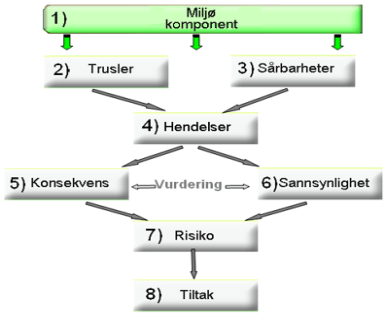
- Personlig informasjon.
- Helseinformasjon.
- Finansiell informasjon.
- Virksomhetssemsitiv informasjon.
- Materielt utstyr som for eksempel PC.

Verdier hos en tjenesteleverandør

- Personlig informasjon.
- Virksomhetsspesifikk informasjon.
- Kunders informasjon.
- Materielt utstyr som for eksempel PC.

Trusler –
Hvem og hva er vi ”redd” ?

Prinsipp for gjennomføring av en risikovurdering



Trusselbildet

• Den teknologiske utviklingen skaper uunngåelig utilsiktede og uønskede virkninger.

• *Truslene* øker i antall og kompleksitet.

• *Trusselbildet* for den enkelte er mer eller mindre i konstant endring.

• Større informasjonssystemer og spesielt informasjonsinfrastrukturer har svakheter som gjør dem *sårbare* for kjente eller ukjente trusler.

Trusler (1)

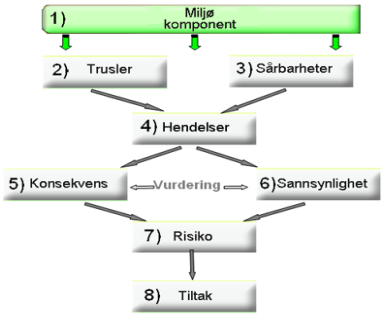
- Virus og annen ondsinnet kode.
- En hacker som kommer seg inn på en ansatts PC eller på en server og legger igjen for eksempel en trojansk hest.
- En hacker som stjeler informasjon fra en ansatts PC eller server.
- En tyv som stjeler en ansatts PC for eksempel når den ligger i bilen.
- Spam som får mail-systemet til å kollapse.
- Denial-of-Service angrep som fører til at vi ikke får tilgang til tjenester på nettet som for eksempel elektronisk valg, selvangivelse eller nettbank.
- Ansatte som bruker msn eller hører på radio over nettet i arbeidstiden.
- Ansatte som bruker bedriftens nettverk til å laste ned porno.
- Uautoriserte som bruker ditt usikrede trådløse nettverk for å spare kostnader for seg selv.
- At noen bruker ditt usikrede trådløse nettverk for å laste ned barneporno.
- At noen bruker bedriftens nettverk og PC’er som utgangspunkt for hacke seg inn på andres maskiner.

Trusler (2)

- Ukjent programvare som fører til at PC’en kræsjer når den installeres.
- Manglende rutiner som medfører at servere blir fulle (av informasjon).
- At PC’en kneler som følge av at jeg søler kaffe i tastaturet.
- At noen får tilgang til opplysninger om vårt kredittkort vårt etter at vi har brukt dette for å betale for vare kjøpt via Internett.
- At noen tapper kontoen vår for penger via vår nettbank.
- At noen utgir seg for å være noen andre for eksempel vha en mail, og prøver å lure mottaker til å gi fra seg virksomhetskritisk informasjon (phishing).
- At noen, uten samtykke, legger ut private bilder av oss på Internett.
- At ansatte laster ned og tar i bruk ulovlig programvare.
- osv.

Sårbarheter –
Hvorfor har vi grunn til å være ”engstelige” ?

Prinsipp for gjennomføring av en risikovurdering



Sårbarheter (1)

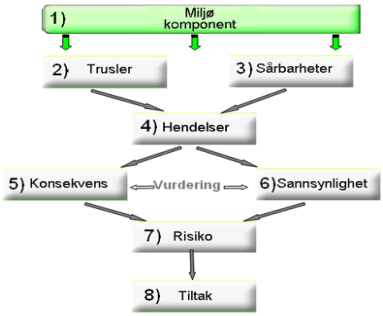
- **Feil i programvare**
  - All programvarekode over et visst antall linjer inneholder feil.
  - Jo flere kodelinjer og kompleksitet, jo flere feil.
- **Systemtekniske sårbarheter**
  - Det finnes ikke noen system som er 100% sikkert.
  - Krever hyppige oppdateringer for å være tilstrekkelig beskyttet.
- **Utstyr blir mindre, mer mobilt og lagringskapasiteten øker**
  - Utstyr mistes eller blir frastjålet.
  - Informasjon blir kopiert fra et medium til et annet.
- **Menneskelige ”sårbarheter”**
  - Vi er naive, og vi liker å være snille og hjelpsomme.
  - Vi tenker ikke på konsekvenser ved å gi fra oss sensitiv informasjon.
  - Vi snakker høyt i mobiltelefon om sensitive ting på tog, flyplass, pub eller liknende.

Sårbarheter (2)

- **Uklare ansvarsforhold**
  - Vi vet ikke hvem som har ansvar for hva for eksempel hvem skal ”patche” en server.
  - Hvem må kjenne til krav til informasjonssikkerhet i rettslige regelverk.
- **For dårlig fysisk sikring**
  - Vinduer lukkes ikke før vi går hjem om kvelden.
  - Bærbar PC blir liggende igjen i bil.
- **For dårlig informasjon og opplæring**
  - Få eller ingen kjenner til policy og andre regler for informasjonssikkerhet.
  - Ikke tilstrekkelig opplæring i policy og regler for bruk av IKT-systemer.

Uønskede hendelser

Prinsipp for gjennomføring av en risikovurdering

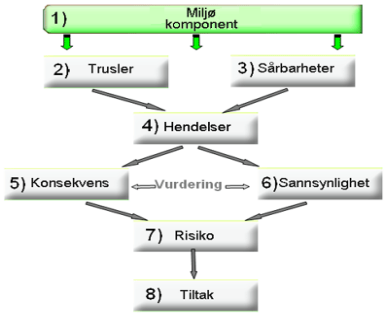


Hva er en uønsket hendelse

- En uønsket hendelse inntreffer når en trussel benytter seg av en eller flere sårbarheter og dette medfører eller kan medføre skade på og/eller tap av en av våre verdier.

Vurdering av konsekvens og sannsynlighet

Prinsipp for gjennomføring av en risikovurdering



Vurdering av konsekvens

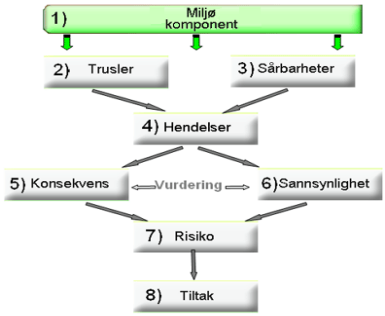
- Vurdering av konsekvens betyr å gjøre en kvalifisert vurdering av hvilke følger en uønsket hendelse som inntreffer kan få.
- Finnes ikke noe fasitsvar for hvordan man skal gjennomføre vurderingen av konsekvens.
- Kan gjøres ved å definere forskjellige konsekvensnivåer.
- Datatilsynet har i sin metode delt inn i følgende nivåer:
  - Katastrofal, stor, moderat og liten.
  - Nivåene kan omgjøres til kvantitative størrelser (for eksempel 4,3,2,1).
- Intervjuer med relevante personer må gjennomføres.

Vurdering av sannsynlighet

- Vurdering av sannsynlighet betyr å gjøre en kvalifisert vurdering av hvor sannsynlig det er at en uønsket hendelse skal inntreffe.
- Ulike tilnærminger må benyttes for eksempel basert på historikk og ”letthet”.
  - Historikk er erfaringsdata.
  - Med ”letthet” menes hvor lett det er for den uønskede hendelsen å inntreffe.
- Kan gjøres ved å definere forskjellige sannsynlighetsnivåer.
- Datatilsynet har i sin metode delt inn i følgende nivåer:
  - Svært høy, høy, moderat og lav.
  - Nivåene kan gis kvantitative størrelser (for eksempel 4,3,2,1)
- Intervjuer med relevante personer må gjennomføres.

Vurdering av anslått risiko

Prinsipp for gjennomføring av en risikovurdering



Vurdering anslått risiko

- Vi har tidligere sagt at anslått risiko er produktet av sannsynlighet og konsekvens.

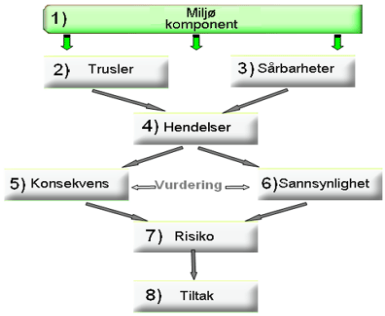
Sannsynlighet * Konsekvens = Anslått risiko.

Risikomatrise - Eksempel

Konsekvens						
	Meget Høy	Middels	Høy	Meget Høy	Meget Høy	Meget Høy
	Høy	Middels	Middels	Høy	Meget Høy	Meget Høy
	Middels	Lav	Middels	Middels	Høy	Meget Høy
	Lav	Lav	Lav	Middels	Middels	Høy
	Meget Lav	Lav	Lav	Lav	Middels	Middels
PRIORITERINGS MATRISE		Meget Lav	Lav	Middels	Høy	Meget Høy
		Sannsynlighet				

Implementering av relevante og nødvendige tiltak

Prinsipp for gjennomføring av en risikovurdering



Implementering av relevante tiltak

- Anslått risiko må sammenliknes med akseptabel risiko.
- Dersom anslått risiko er høyere enn akseptabel risiko, må det gjøres enn vurdering av om det skal implementeres tiltak.
  - Kostnader er en viktig faktor.
  - Hvilke risiko er man villig til å "leve" med?
- Tiltak kan være av flere typer:
  - Fysiske (inngangskontroll, låste datarom)
  - Juridiske (taushetserklæringer)
  - Organisatoriske (Tydeliggjøring av roller, ansvar og myndighet, rutiner)
  - Teknologiske (Antivirus, brannmur, patching av OS)
  - Pedagogiske (Informasjon og opplæring, holdningskampanjer)