Krav til informasjonssikkerhet

DRI1010 – forelesning 08.03.2017

Jon B. Holden – jobe@holden.no

Vault 7: CIA Hacking Tools Revealed

A series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

Dagens tema: Informasjonssikkerhet + internkontroll

- Krav til informasjonssikkerhet og internkontroll i
  - Personopplysningsloven, -forskriften
  - Eforvaltningsforskriften
  - Andre regelverk

Informasjonssikkerhet, pol § 13

- **§ 13.** *Informasjonssikkerhet*
- Den behandlingsansvarlige og databehandleren skal gjennom **planlagte og systematiske** tiltak sørge **for tilfredsstillende informasjonssikkerhet** med hensyn til **konfidensialitet, integritet og tilgjengelighet** ved behandling av personopplysninger.
- For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren **dokumentere** informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
- En behandlingsansvarlig som lar **andre** få tilgang til personopplysninger, **f.eks. en databehandler eller andre som utfører oppdrag** i tilknytning til informasjonssystemet, skal **påse at disse oppfyller kravene** i første og annet ledd.
- Kongen kan gi **forskrift** om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Personopplysningslovens krav

- Hva skal sikres?
  - Vern av konfidensialitet, integritet og tilgjengelighet for personopplysninger, pof § 2-1
- Hvem skal sikre?
  - Den behandlingsansvarlige og databehandleren, § 13
- Hvor sikkert?
  - Tilfredsstillende, jf. § 13 = forholdsmessig, pof § 2-1
  - Risikovurdering, jf. pof § 2-4
  - Behandlingsansvarlig avgjør nivå, ev. Datatilsynet, jf. pof § 2-2

Hva skal sikres?

- Konfidensialitet
  - Vern mot uautorisert innsyn
- Integritet
  - Vern mot uautorisert endring/tap
- Tilgjengelighet
  - Tilgjengelig på behov

Praktisk øvelse – vurder K, I, T tilsiktet/utilsiktet

Hvem har ansvaret?

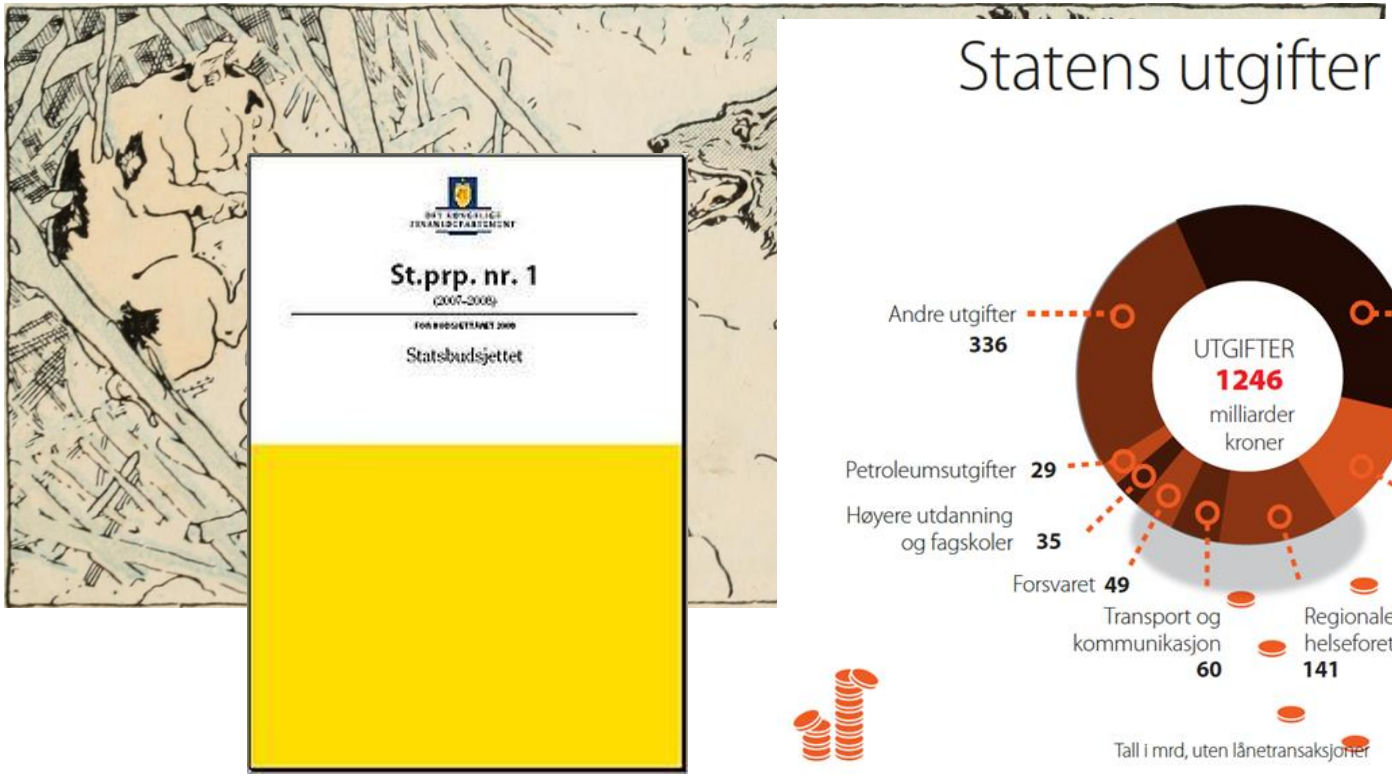
- Den behandlingsansvarlige

- Databehandleren
  - Selvstendig ansvar, men innen rammen som settes av den beh.ansvarlige

Hvordan sikre?

- Systematisk, dokumentert arbeid
  - Bl.a. sikkerhetsmål, -strategi, revisjoner (§§2-3 – 2-5), 5 års lagring §2-16 mfl
- Organisatoriske, tekniske tiltak
  - Eks. pof §§ 2-11 – 2-13 pålegger tiltak *hvis nødvendig*
  - Følge opp databehandlere (”påse”, pol § 13 tredje ledd)

Hvor sikkert?

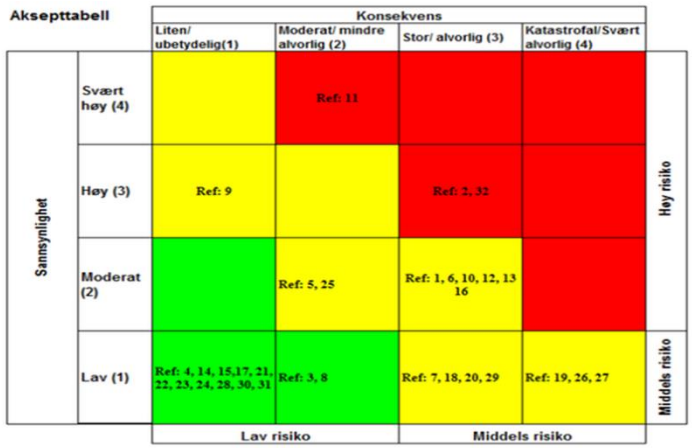


HVORDAN FINNE RIKTIG NIVÅ?


Skjermlås
Hvitliste
Sikkerhetskopier
Fjellhall
Adgangskontroll
Opplæring
Brannmur
AUTENTISERING
Kryptering
Redundans
Ansvarsdeling
IKT-instruks
Overvåking
Sikkerhetsansvarlig
Beredskapsplan
Ytelsestest
Logging

Risikovurdering - prioritering av tiltak

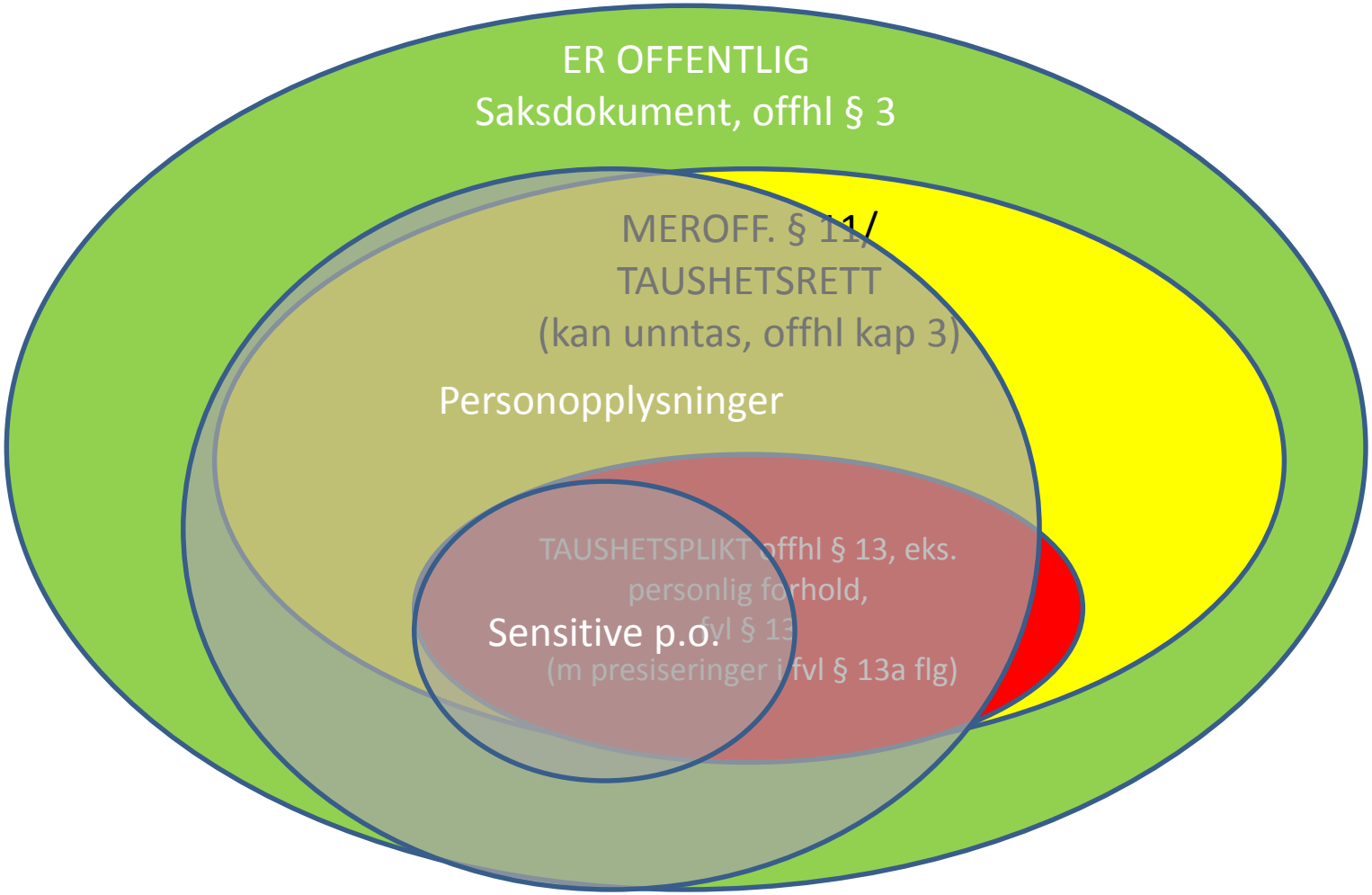
- Mange metoder
- Veiledning fra Datatilsynet og Difi
  - Kartlegge opplysningstyper
  - Identifisere uønskede hendelser
  - Vurdere konsekvenser og sannsynligheter
  - Innplassering i risikomatrise
  - Valg av tiltak



Kartlegging

- Konfidensialitet - innsynsvern
  - Uvedkommendes bruk/innsyn
  - Taushetsplikt vs. offentlighet
- Integritet - endringsvern
  - Betydning for vedtak, avgjørelser
- Tilgjengelighet - tilgangsvern
  - Tidskritisk?

Kartlegging - konfidensialitet



Identifisere og analysere hendelser

- Identifisere uønskede hendelser
  - Villede og uaktsomme handlinger, hendelige uhell og naturfenomener
- Vurdere konsekvenser for hendelsene
- Vurdere sannsynlighet for hendelsene
- = Risiko

Eksempler på hendelser

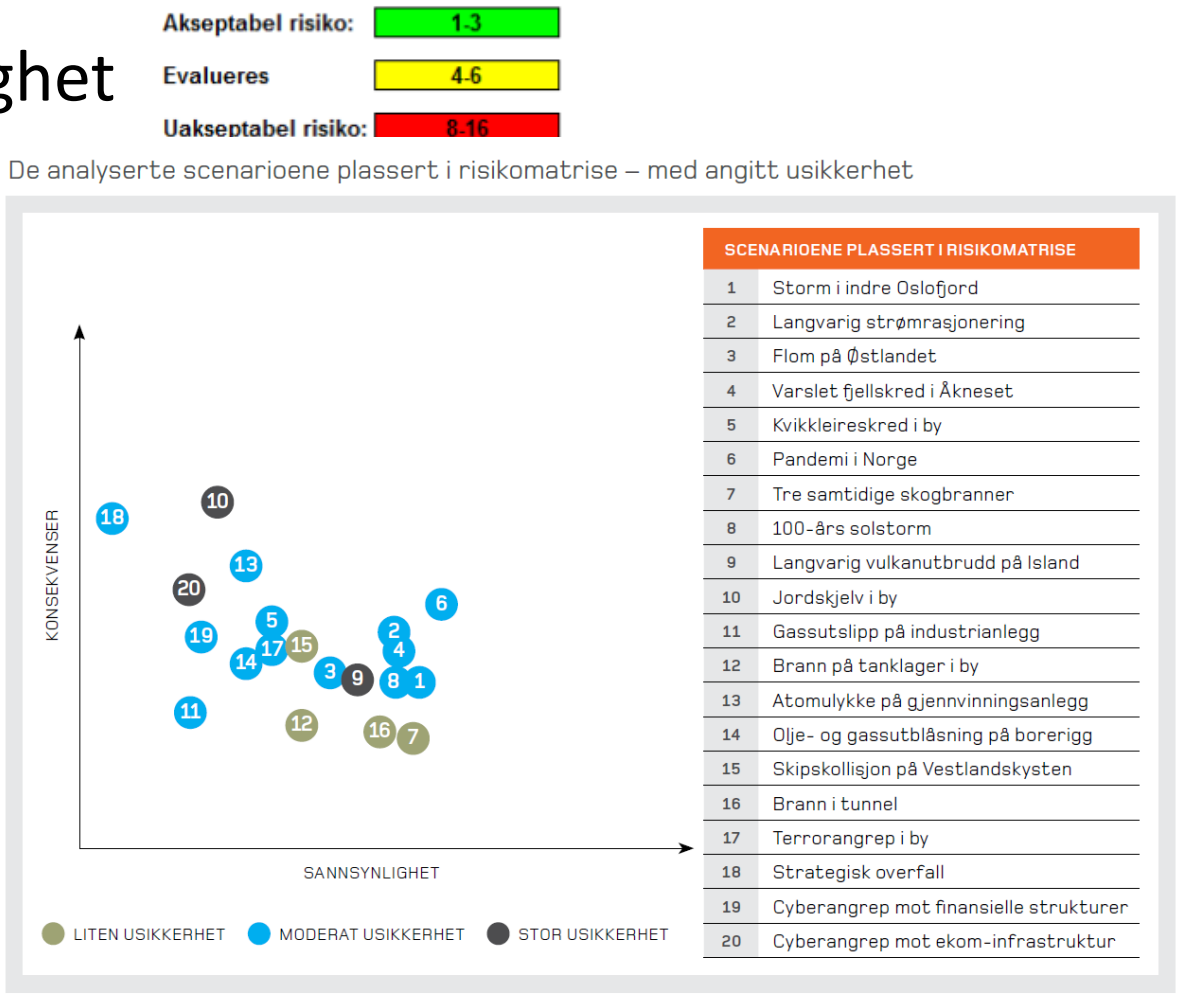
- Hacking av nettløsning – publiserer opplysningene
- Hacking av nettløsning – endrer utbetalingskonto
- Utro tjener selger opplysninger om Kongehuset til pressen
- Datahallen brenner – opplysningene mistes
- Datahallen brenner – tjenesten er utilgjengelig

Vurdering av skade og sannsynlighet

- Egne og andre erfaringer
  - Tilfeldige hendelser
  - Tilsiktede hendelser
- Trusselaktører - hvem har nytte av opplysningene?
  - Motivasjon til misbruk
  - Gevinst av misbruk
- Kan skaden heles?

Risikomatrise

- Risiko: sannsynlighet konsekvens
- Akseptabelt risik fastsettes
- Konsekvenser
- Sannsynlighet vu
  - Letthet, motivas kapasitet, frekve
- Eksempler: Bo Nasjonalt risik 2014 (s205)



FIGUR 22. Nasjonalt risikobilde – samlet risikomatrise viser vurdert risiko (sannsynlighet, konsekvens og usikkerhet) knyttet til de konkrete alvorlige scenarioene som er analysert.

Eksempler på sikkerhetstiltak

- Krav til innlogging
  - Passord, MinID, BankID, smartkort, biometri (fingeravtrykk, ansiktsgeometri), etc
- Tilgangsstyring (need-to-know vs. need-to-hide)
- Krav til logging, gjennomgang av logger
- Backup, reserveløsninger
- Kryptering, tempest-vern, forsvarlig sletting
- Sikkerhetstesting (innbruddstest)
- Revisjon, pof § 13

Direktivet

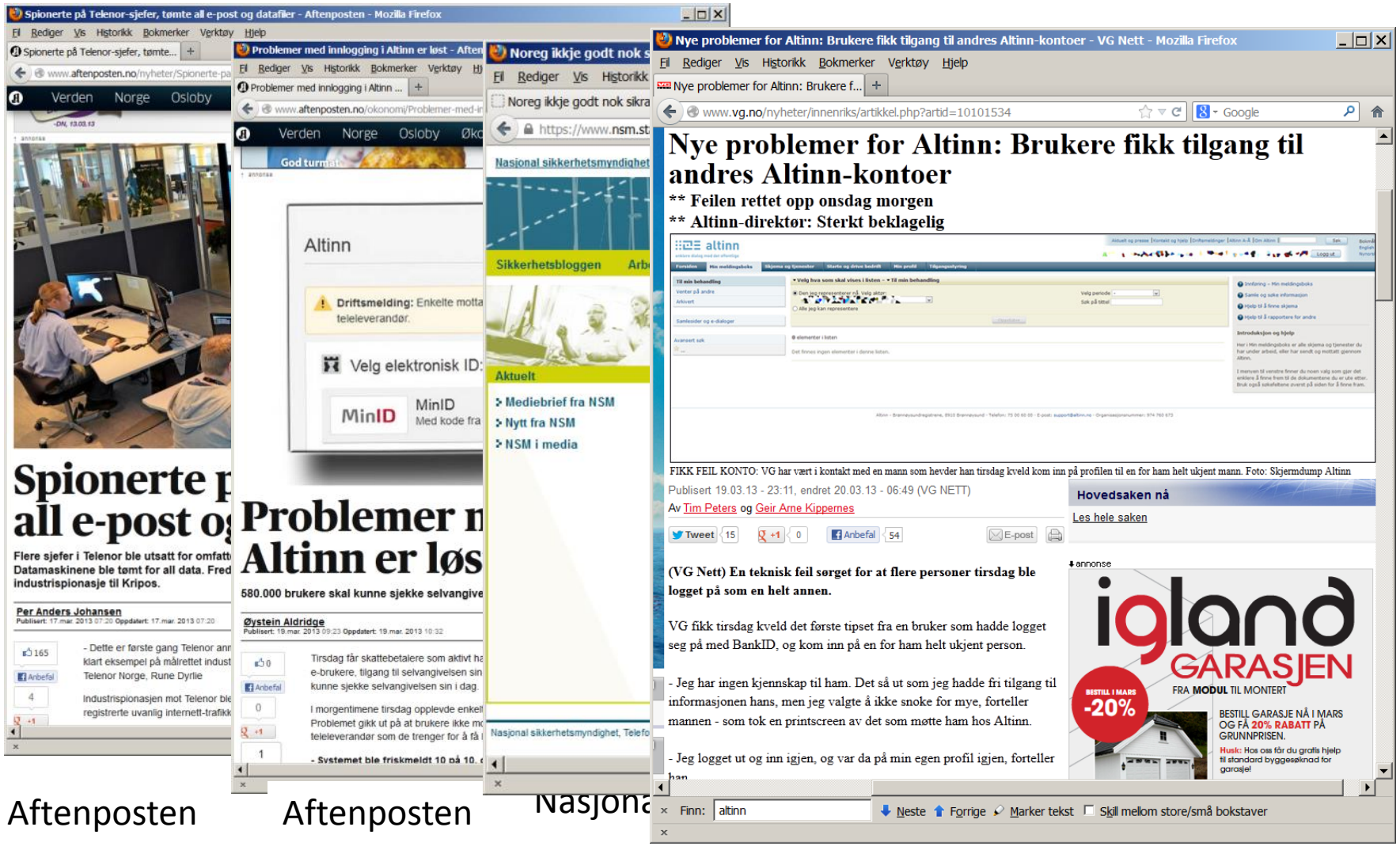
- Behandlingssikkerhed, artikkel 17:
  - 1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de **fornødne tekniske og organisatoriske foranstaltninger** til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for **ulovlig behandling**.
  - **http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:31995L0046#texte**

Krav til informasjonssikkerhet, i personvernforordningen (2016/0679)

- Artikkel 32
  - 1. Under hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysisk personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et **sikkerhedsniveau**, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:
    - ...
  - 2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling af oplysninger udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

...

Vurder oppslagene



Aftenposten Aftenposten Nasjona

VG

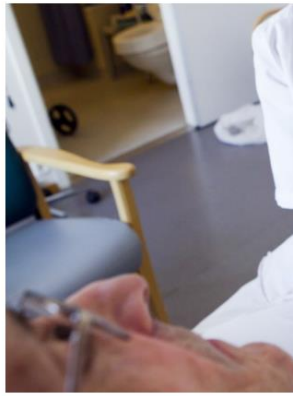
Informasjonssikkerhet i media

NRK NYHETER SPORT TV RADIO DISTRIKT

Norge Siste nytt Dokumentar Klima

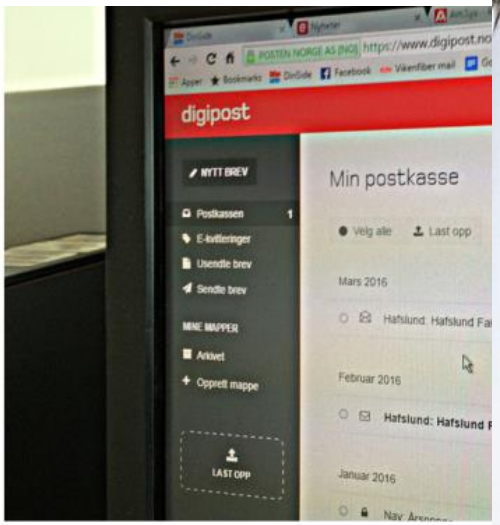
Ny rapport: Al kommunene

Mangler eller feil i pasienters helseinforr ut for tidlig. Dette er noen av funnene i e Helsetilsynet.



SKRIVES UT TIDLIGERE FRA SYKEHUS: Fastleger helsetilstand og behov for hjelp når pasienter skrives u
FOTO: JUNGE, HEIKO / NTB SCANPIX

Tirsdag offentliggjorde Helsetilsyne Norge etter at samarbeidsreformer



SIKRERE: Både e-Boks og Digipost tilfredsstiller kravene, men Digipost har sikkerhetsrådgiveren Per Thorsheim. (Foto: TORE NESET)

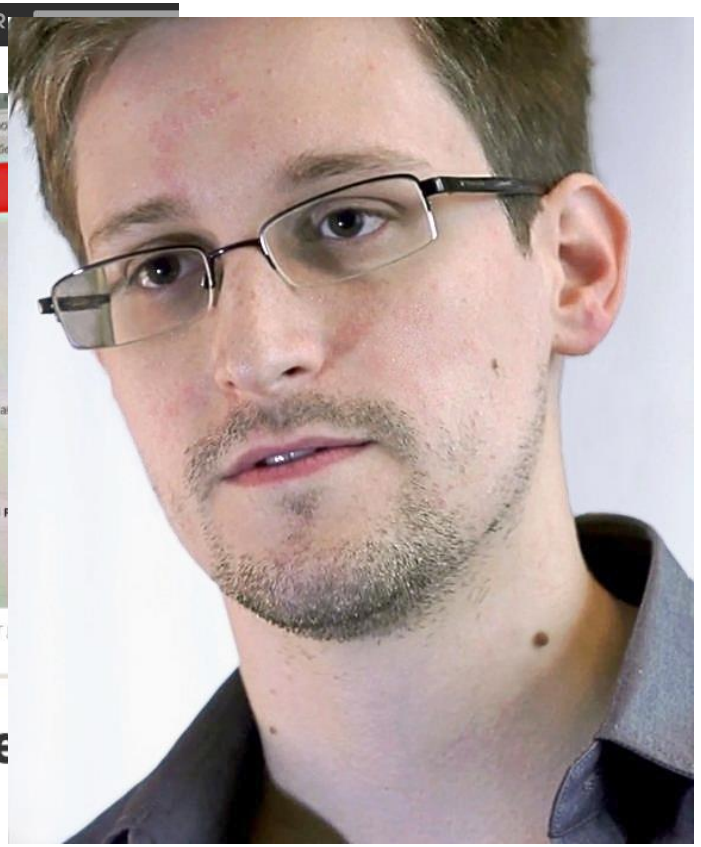
- Digipost er sikrere

24

Det mener sikkerhetseksrådgiveren Per Thorsheim.

Dinside Onsdag denne uka gjorde Dinside en sammenligning mellom de to digitalpostkassene Digipost og e-Boks.

av Tore Neset



Publisert: Torsdag 10. mars 2016 kl 17:00

Annonse

Internkontroll, pol § 14

- **§ 14.** *Internkontroll*
- Den behandlingsansvarlige skal etablere og holde vedlike **planlagte og systematiske** tiltak **som er nødvendige** for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes **kvalitet**.
- Den behandlingsansvarlige skal **dokumentere** tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
- Kongen kan gi **forskrift** med nærmere regler om internkontroll.

Krav til internkontrollen, § 14

- Planlagt og systematisk
- Tiltak som «er nødvendig»
- Dokumentert
  - For medarbeidere og tilsynsmyndigheter

Eksempler på internkontrolltiltak

- Opplæring
- Rutinebeskrivelser (innsyn, informasjonsplikt, ny behandling, sletting)
- Revisjon

Krav til internkontroll, personverforordningen artikkel 24

Artikel 24

Den dataansvarliges ansvar

1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.
2. ...

Sikkerhetskrav i forvaltningsloven / eforvaltningsforskriften

- **Fvl § 13** om taushetsplikt
  - **hindre** at andre får adgang eller kjennskap… § 13
  - forsvarlig oppbevaring, § 13c annet ledd
  - informerte medarbeidere, § 13c første ledd

FORVALTNINGSLOV OG EFVF

Eforvaltningsforskriften

- Opprinnelig fra 2002
- Viktige endringer 2014 – digitalt førstevalg
- Hjemlet i forvaltningsloven § 15a (og esignl)
- Formål, § 1:
  - **sikker og effektiv bruk** av elektronisk kommunikasjon med og i forvaltningen
  - **forutsigbarhet**, fleksibilitet, samordning av løsninger
  - enhver på en **enkel måte** kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige

efvf og informasjonssikkerhet

- Overordnet krav til **internkontroll** på informasjonssikkerhetsområdet, § 15
  - Basert på anerkjente standarder for styringssystem for informasjonssikkerhet
  - Mål og strategier, ref. pof § 2-3
  - Omfang basert på **risiko**, ref. pof § 3-1
  - Fortrinnsvis helhetlig styringssystem
- Publikums digitale kommunikasjon med forvaltningen
  - Kan skje uten bruk av sikkerhetstjenester, med mindre det kreves, § 4
    - Organet må tilby eller peke på løsninger, § 4 nr 4
  - Regulering av innkommende taushetsbelagte opplysninger fra publikum, § 5
- Efvf kap 4-6 – regulering av sertifikater og private nøkler

Efvf § 15

- § 15. *Internkontroll på informasjonssikkerhetsområdet (utdrag: annet og tredje ledd)*
  - Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på **anerkjente standarder** for styringssystem for informasjonssikkerhet. Internkontrollen **bør** være en **integrert del** av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi **anbefalinger** på området.
  - Omfang og innretning på internkontrollen skal være **tilpasset risiko**.
- Veiledning: internkontroll.infosikkerhet.difi.no

Digital kommunikasjon til innbyggerne

- Digitale **meldinger** til innbyggerne
  - Kan sendes, efvf § 8
  - Strengere krav til enkeltvedtak og andre viktige meldinger
    - Egnet informasjonssystem (hovedregel)
    - Varsel, gjentatt varsel
    - Logging av innsyn
  - Innbygger kan reservere seg mot å få viktige meldinger, § 9

- Digital **kontaktinformasjon** til innbyggerne
  - Kan lagres, efvf § 31
  - Opprettes med opplysninger fra ID-porten, § 38
  - Kan brukes i forvaltningen, varsling § 29

Et fellestrekk: risikobaserte krav

- «tilfredsstillende», «nødvendige» tiltak
  - pol §§ 13, 14
- «passende» tiltak
  - personvernforordningen art 24 og 32
- omfang og innretning «tilpasset risiko»
  - eforvaltningsforskriften § 15

Andre regelverk med krav til informasjonssikkerhet

- Egne taushetspliktsbestemmelser i sektorlover
  - NAV-loven § 7, skatteforvaltningsloven § 3-1
- Generelle regler for beskyttelse mot særlig alvorlige skader
  - Sikkerhetsloven & informasjonssikkerhetsforskriften, objektsikkerhetsforskriften
  - Beskyttelsesinstruksen (kun statsforvaltningen)
- Internkontrollkrav i økonomiregelverket for staten
- Annen særregulering
  - Helseregisterloven, ikt-forskriften

Eksempel på krav til sikring

§ 7-36.Sikring av kryptorom

… Dører til kryptorom skal være av minimum 40 millimeter heltre eller tilsvarende styrkenivå og være forsvarlig montert. Dersom døren er utvendig hengslet, skal den sikres i bakkant.

Veggene skal gå fra gulv til fast tak og skal ikke kunne demonteres fra utsiden uten at det avsettes spor. I rom med nedsenket himling skal område mellom himling og tak være kontrollerbart.

…

§ 7-37.Adgangskontroll

Det skal gjennomføres kontroll med adgangen til kryptorom. For adgang kreves kryptoautorisasjon. Det skal foreligge en liste over personell som har permanent adgang. Listen skal signeres av **virksomhetens leder**. Bare én dør skal benyttes for inn- og utpassering. Andre dører skal være forsvarlig sikret mot inntrenging og skal bare kunne åpnes fra innsiden. Besøkende med tjenstlig behov kan få adgang dersom det er godkjent av virksomhetens leder og de ledsages av personell med permanent adgang. Besøkende skal **legitimere seg** og registreres i protokoll eller lignende besøksregister. Besøksregisteret skal **bevares i minst ti år.**

I områder hvor det oppbevares store mengder kryptonøkler eller hvor det kryptonøkler produseres eller administreres, skal det etableres adgangsrutiner som sikrer at det **alltid er to kryptoautoriserte** personer til stede samtidig.

https://lovdata.no/forskrift/2001-07-01-744/§7-36

Kort om sikkerhetsloven

- Formål, jf. § 1
  - ”motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser…”
- Gradering, § 11 – STRENGT HEMMELIG/ HEMMELIG/ KONFIDENSIELT/ BEGRENSET
  - Skade hvis informasjonen kommer på avveie (ref. § 1)
- Streng need-to-know, § 12
- NSM-godkjenning av informasjonssystemer, § 13, m.v.
- Forskrifter
  - Informasjonssikkerhetsforskrift m.v. med detaljerte sikringsregler
  - Objektsikkerhetsforskriften

Kort om beskyttelsesinstruksen

- Instruks for statsforvaltningen
- Gradering (§ 2)
  - STRENGT FORTROLIG eller FORTROLIG
- Vurderingstema (§ 4)– skade/betydelig skade mht.
  - offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende
- Konsekvenser
  - Strengt need-to-know-prinsipp, § 7 – personlig ansvar
- Elektronisk behandling ”så langt det passer” ihht. deler av informasjonssikkerhetsforskriften etter sikkerhetsloven, jf. § 12

- Spørsmål?