

Krav til informasjonssikkerhet

DRI1010 – forelesning 25.03.2015

Jon B. Holden – jobe@holden.no

Dagens tema: Informasjonssikkerhet og eforvaltningsforskriften

- Hva er informasjonssikkerhet?
- Krav til informasjonssikkerhet og internkontroll etter pol
- Eforvaltningsforskriften

Informasjonssikkerhet i media

Spionerte på Telenor-sjefer, tømte all e-post og datamaskinene ble tømt for all data. Fred industrispionasje til Kripos.

Problemer med innlogging i Altinn er løst

Nye problemer for Altinn: Brukere fikk tilgang til andres Altinn-kontoer

**** Feilen rettet opp onsdag morgen**

**** Altinn-direktør: Sterkt beklagelig**

VG har vært i kontakt med en mann som hevder han tirsdag kveld kom inn på profilen til en for ham helt ukjent mann. Foto: Skjermdump Altinn

Publisert 19.03.13 - 23:11, endret 20.03.13 - 06:49 (VG NETT)

Av [Tim Peters](#) og [Geir Arne Kippernes](#)

Tweet (15) +1 (0) Anbefal (54) E-post

Hovedsaken nå

[Les hele saken](#)

igland GARASJEN

BESTILL I MARS -20%

FRA MODUL TIL MONTERT

BESTILL GARASJE NÅ I MARS OG FÅ 20% RABATT PÅ GRUNNPRISEN.

Husk: Hos oss får du gratis hjelp til standard byggeskred for garasje!

Aftenposten 17.3 Aftenposten 18 Nasjon

VG 20.3.2013

Informasjonssikkerhet i media

altinn
Direktoratet for forvaltning og IKT

OFFENTLIGE ANSKAFFELSER

28 Jan 2014 10:24:42 3 Days 19:2

Home Configuration

AA59 NO PL

XXF NO PL

NO PL

NO PL

NO PL

Et slikt skjermbilde møtte Stangvik da han fant siden h

Kamera so på gamleve åpent ute p

Dersom du visste nettadressen, kunne som krysset svenskegrensen på Fylkes

Arild Færaas
Oppdatert: 23. mar. 2014 19:20



PST adv:
– Vi har ikke nasjonal ko

Mandag 10. februar 2014 kl.
Av Norsk Telegrambyrå

Politiets sikkerhetstjeneste myndighetene ikke har god norske telekommnetet, hvor er dypt inne i utbyggingen.

– Det er et problem at sels ikke har sikkerhetssamarb seksjonssjef Erik Hauglanc

Han sikter til det kinesiske som har fått oppdraget mer deler av nettet nordmenn b elektronisk kommunikasjor han nå advarselen PST, No Sikkerhetsmyndighet (NSN Etterretningstjenesten kom

– Som andre lands sikkerh bekymret for at vi ikke har vårt eget ekomnett. Vi men man sørge for å ha et sikke det landet som den aktører



STOPPET OPP: 17-åringen hacket en rekke av landets største nettsider. DNB alene varslet millioensaks mål i etterkant.

Hacker (17) slipper å betale 400.000 kr

■ **Må jobbe 150 timer**

Skoleelev fra Bergen parkere en rekke av landets største nettsider, men trenger ikke å betale erstatning.

Frøde Buanes, Guro Valland, Audun Hageskal

Publisert: 26 feb. 2015 18:43 Oppdatert: 26 feb. 2015 18:59

Lagre i leselisten

Lagret i leselisten

I juli i fjor ble en 17-åring i Åsane pågrepet og siktet for å ha gjennomført omfattende dataangrep mot flere av Norges største bedrifter.

Nå er han dømt til samfunnsstraff i 150 timer for ungeringen. Det var BA som

FAKTA

- DDoS er en forkortelse for «Distributed Denial of Service», eller tjenestektangrep på norsk. Det er ikke det samme som et hackerangrep.
- Tjenestektangrep har til hensikt å hindre tilgangen til tjenestene på et nettsted. Hackerangrep har på sin side som regel til hensikt å ødelegge systemer eller innhente sensitive opplysninger.
- Tjenestektangrep gjennomføres ved at angriperen eller angriperne sender enorme mengder henvendelser til et

Sikkerhet - hva skal beskyttes?

- Informasjonssikkerhet (def. ISO 27001, 3.4)
 - Bevare konfidensialitet, integritet og tilgjengelighet. Dessuten kan andre egenskaper, som autensitet, ansvarlighet, uavviselighet og pålitelighet, omfattes.
- Konfidensialitet
 - Vern mot uautorisert innsyn
- Integritet
 - Vern mot uautorisert endring/tap
- Tilgjengelighet
 - Tilgjengelig på behov

Direktivet

- Behandlingsikkerhed, artikel 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>

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 Personvernemnda.
- 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

Personopplysningslovens krav (forts.)

- 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)

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 Personvernemnda.
- Kongen kan gi **forskrift** med nærmere regler om internkontroll.

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
 - [Helseregisterloven § 13](#) sjette ledd
- Backup, kryptering, forsvarlig destruksjon, vern mot avlytting/tempest, reserveløsning
- Revisjon, pof § 13
- Sikkerhetstesting (innbruddstest)

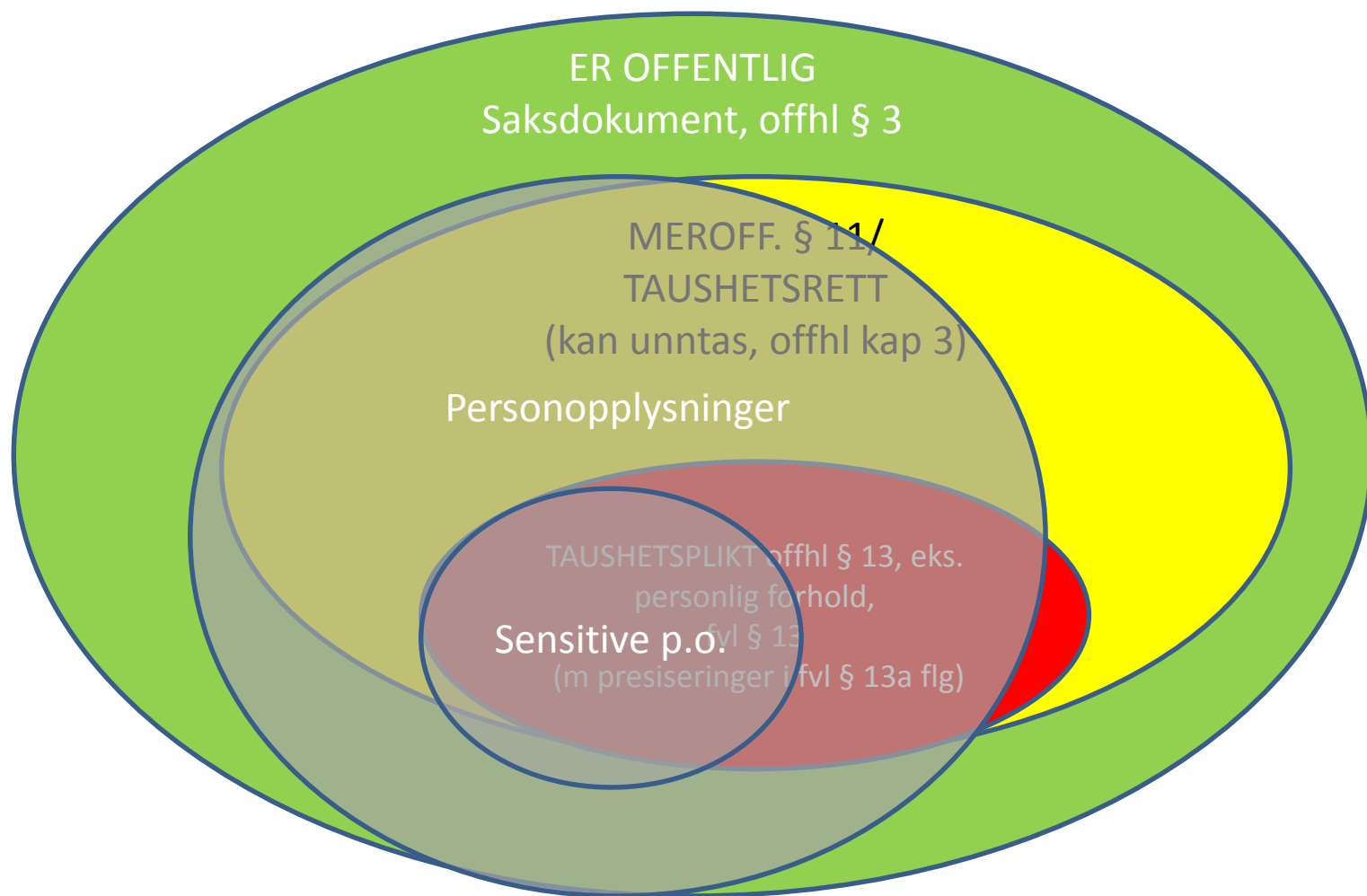
Gjennomføring av risikovurdering

- Mange metoder
- Veiledning fra [Datatilsynet](#) og [Difi](#)
 - Kartlegge opplysningstyper etc
 - 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 - tilgangsværn
 - Tidskritisk?

Kartlegging - konfidensialitet



Identifisere og analysere hendelser

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

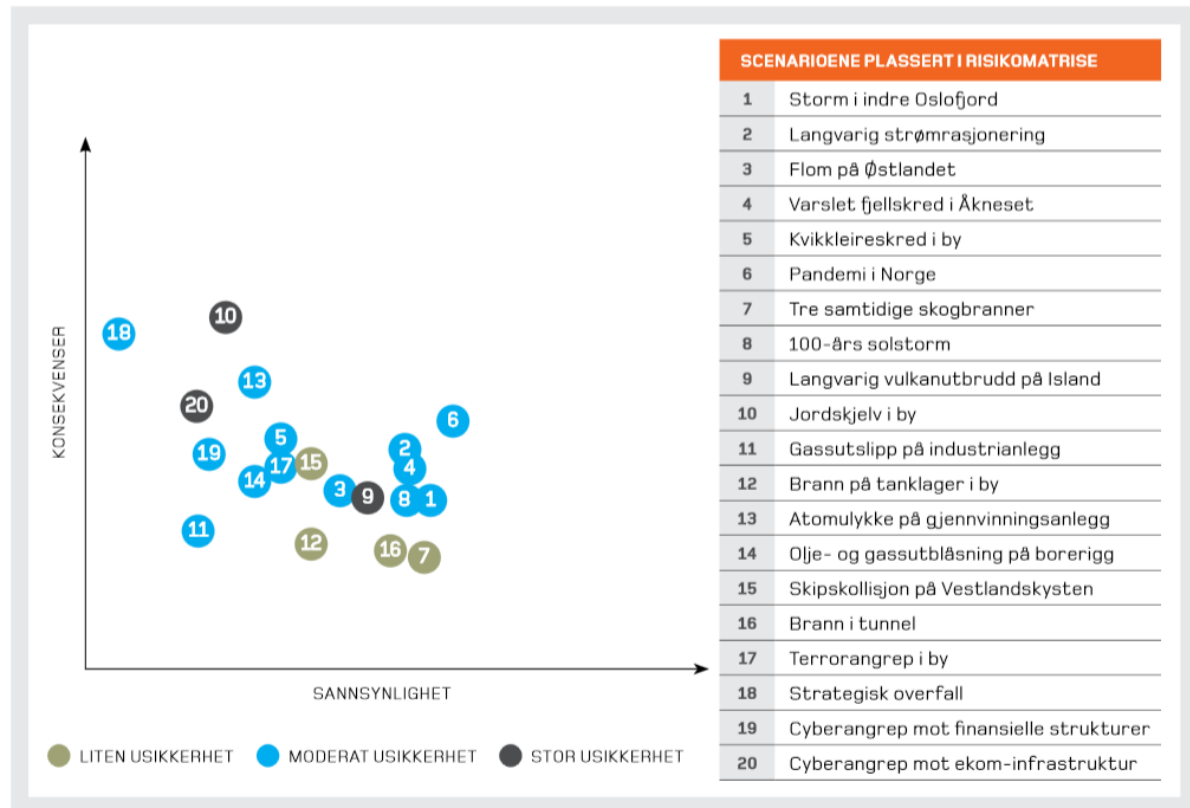
Risikomatrise

- Risiko: sannsynlighet
konsekvens
- Akseptabelt risikon
fastsettes
- Sannsynlighet vurd
– Letthet, motivasjon
kapasitet, frekvens
- Konsekvenser
- Eksempler: [Box, Nasjonalt risikok 2012](#) (s17)

Akseptabel risiko: 1-3

Evalueres 4-6

De analyserte scenarioene plassert i risikomatrise – med angitt usikkerhet



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

Andre regelverk med krav til informasjonssikkerhet

- eforvaltningsforskriften, § 15 m.fl.
- Taushetspliktsbestemmelser
 - [Forvaltningsloven §13](#), [lignl §3-13](#)
 - [Sikkerhetsloven](#) & [informasjonssikkerhetsforskriften](#), [objektsikkerhetsforskriften](#)
 - [Beskyttelsesinstruksen](#) (kun statsforvaltningen)
- [Internkontrollkrav](#)
- Særregulering
 - Helseregisterloven, ikt-forskriften

Forvaltningsloven § 13 flg

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

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

Eforvaltningsforskriften

- Opprinnelig fra 2002
- Viktige endringer 2014 – digitalt førstevalg
- Forankret 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

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

- Spørsmål?

Kort om elektronisk signatur

- [Esignaturloven § 3](#) definerer tre typer e-signaturer
 - Nr 1: (vanlige)
 - Nr 2: Avanserte
 - Nr 3: Kvalifiserte
- Hva kreves?
 - Prosessrettslig, privatrettslig, forvaltningsrettslig utgpkpt
 - Fri bevisbedømmelse, formfrihet, forsvarlig saksbehandling
 - Regelverket gir tidvis avklaring
 - Risikovurdering!
- Merk [efvf § 26](#) nr 2 – langtidslagring
 - arkivet vil kunne bryte signaturen, må da gå god for bindingen
- Revisjon av regelverket på gang – ny forordning vedtatt 2014 ([eIDAS](#))