

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 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

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

Altinn
Direktoratet for forvaltning og IKT

28 Jan 2014 10:24:42 3 Days 19

OFFENTLIGE ANSKAFFELSER

Home Configuration

AA59

XXF

NO P

NO P

NO P

NO P

NO P

NO P

Et slikt skjermbilde møtte Stangvik da han fant sides

Kamera se på gamle åpent ute

Dersom du visste nettdressen, kunn som krysset svenskegrensen på Fylk

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

BankID: 35,9 %



...ske Huawei er hoffleverandør av både Jørgenrud)

PST adva

– Vi har ikke nasjonal kont

Mandag 10. februar 2014 kl. 10
Av Norsk Telegrambyrå

Politiets sikkerhetstjeneste e myndighetene ikke har god n norske telekommettet, hvor ut er dypt inne i utbyggingen.

– Det er et problem at selska ikke har sikkerhetssamarbeid seksjonssjef Erik Haugland i

Han sikter til det kinesiske s som har fått oppdraget med å deler av nettet nordmenn bruk elektronisk kommunikasjon. I han nå advarselen PST, Nors Sikkerhetsmyndighet (NSM) Etterretningsjensetenen kom n

– Som andre lands sikkerhet bekymret for at vi ikke har nasjonal kontroll på vårt eget ekomnett. Vi mener at i det minste må man sørge for å ha et sikkerhetssamarbeid med det landet som den aktøren kommer fra i bunnen,



Hacker (17) slipper å betale 400.000 kr

■ Må jobbe 150 timer

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

Frode Buanes, Guro Valland, Audun Hageskal

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

Lagre 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 tjenestenektangrep på norsk. Det er ikke det samme som et hackerangrep.
- Tjenestenektangrep 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.
- Tjenestenektangrep gjennomføres ved at angriperen eller angriperne sender enorme mengder henvendelser til et nettsted.

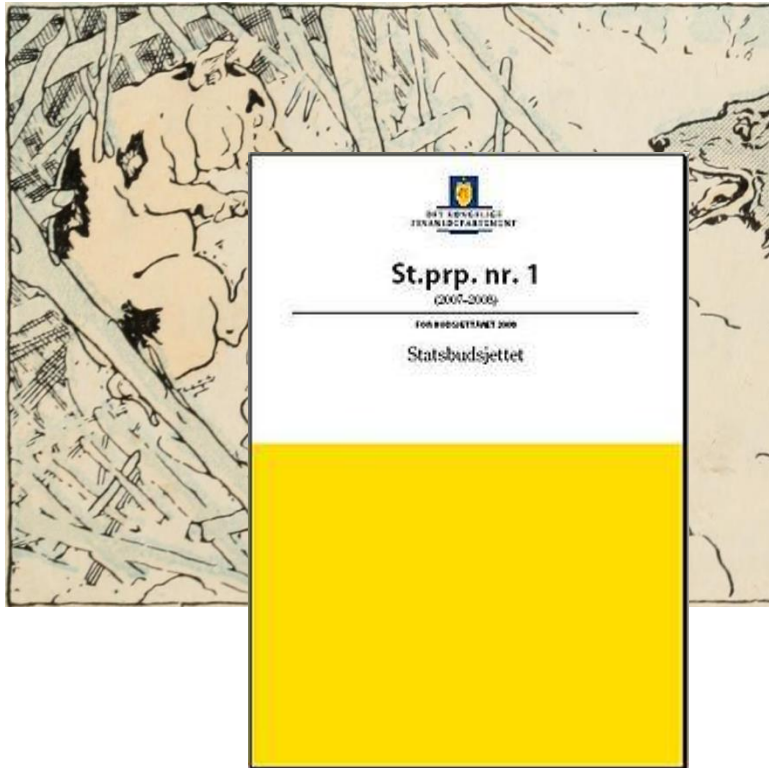
Hvem har ansvaret?

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

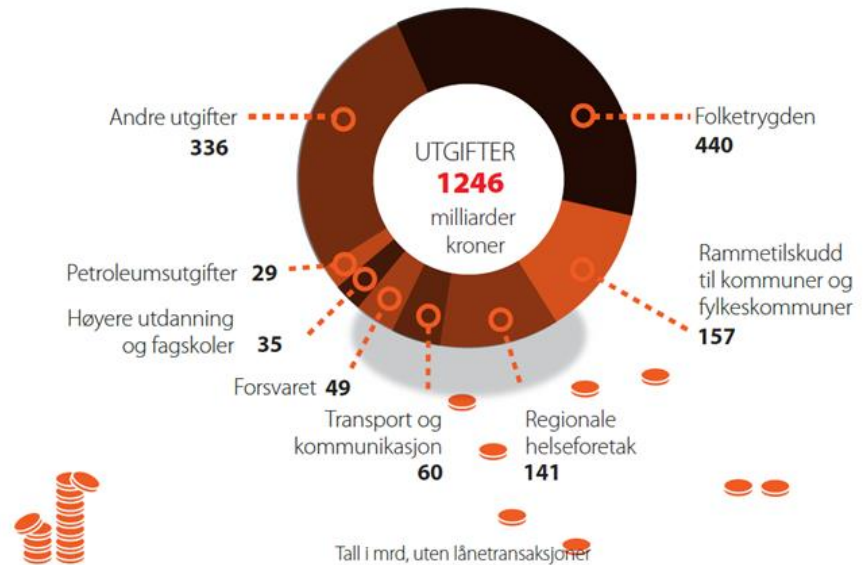
Hvordan sikre?

- 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?



Statens utgifter 2016



HVORDAN FINNE RIKTIG NIVÅ?

Skjermlås

Hvitliste

Sikkerhetskopier

Fjellhall

Adgangskontroll

Opplæring

Brannmur

AUTENTISERING

Kryptering

Redundans

IKT-instruks

Ansvarsdeling

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

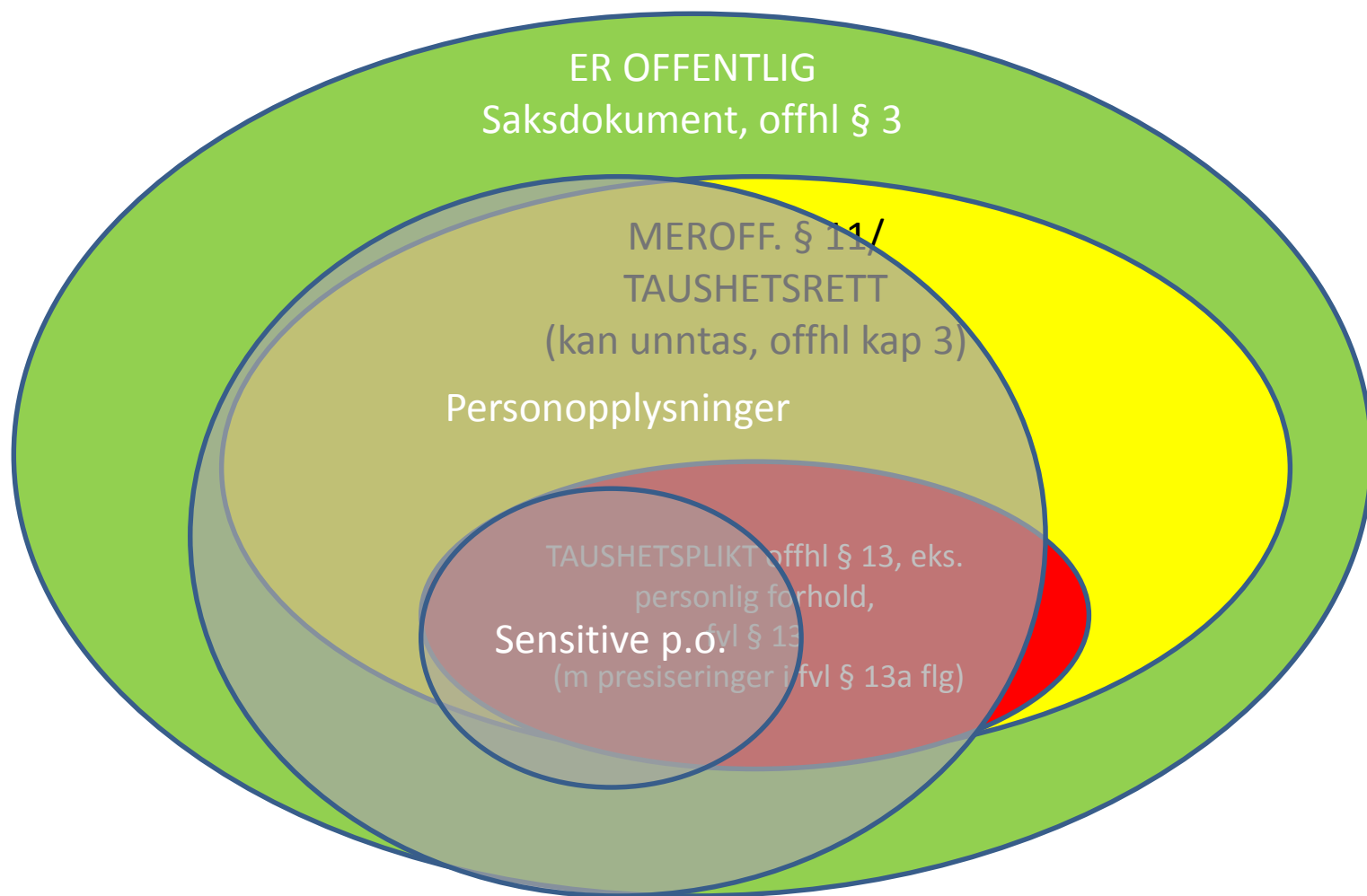
Aksepttabell

| | | Konsekvens | | | |
|---------------|------------------|---|---------------------------------|-----------------------------|-----------------------------------|
| | | Liten/ ubetydelig(1) | Moderat/ mindre alvorlig (2) | Stor/ alvorlig (3) | Katastrofal/Svært alvorlig (4) |
| Sannsynlighet | Svært høy (4) | | Ref: 11 | | |
| | Høy (3) | Ref: 9 | | Ref: 2, 32 | |
| | Moderat (2) | | Ref: 5, 25 | Ref: 1, 6, 10, 12, 13 16 | |
| | Lav (1) | Ref: 4, 14, 15, 17, 21, 22, 23, 24, 28, 30, 31 | Ref: 3, 8 | Ref: 7, 18, 20, 29 | Ref: 19, 26, 27 |
| | | Lav risiko | | Middels risiko | |
| | | Høy risiko | | | |
| | | Middels risiko | | | |

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

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

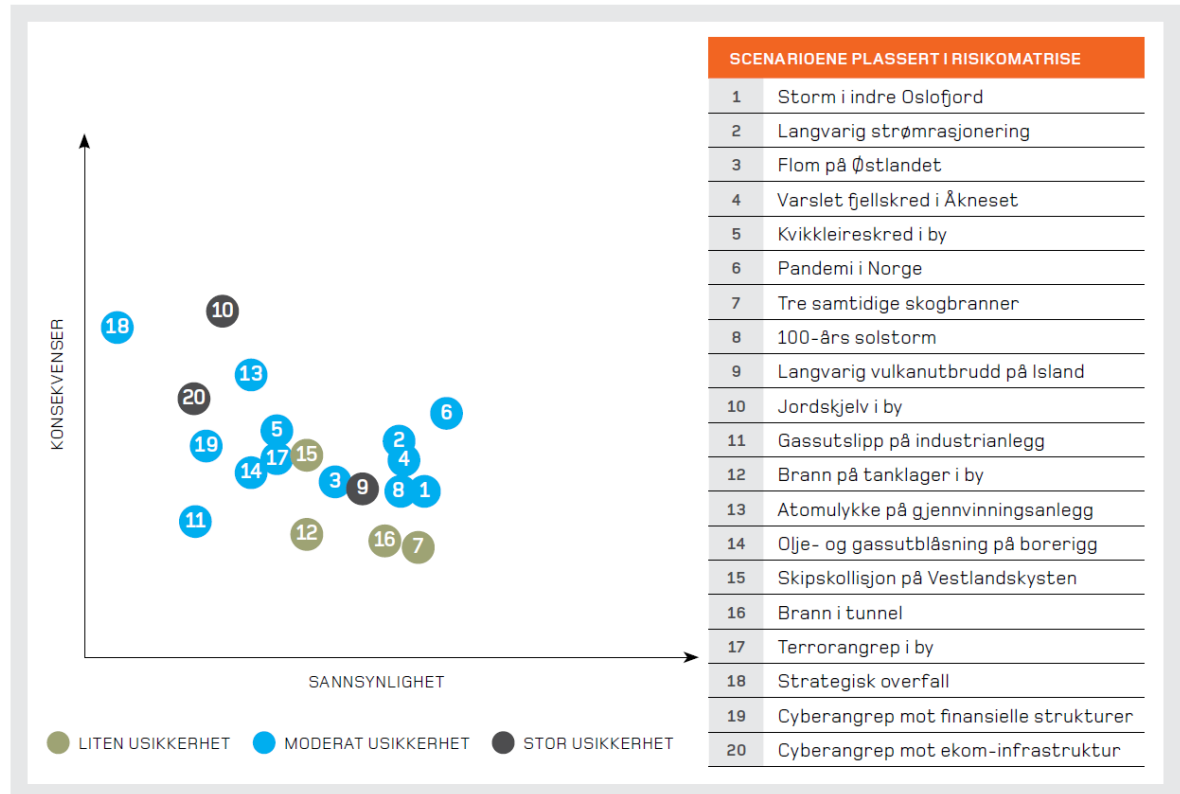
- Egne og andre erfaringer
 - Tilfeldige hendelser
 - Tilsiktede hendelser
- Trusselaktører - hvem har nytte av opplysningene?
 - Motivasjon til misbruk
 - Gevinst av misbruk
- Kan skaden heles?

Risikomatrise

- Risiko: sannsynlighet
konsekvens
- Akseptabelt risiko
fastsettes
- Konsekvenser
- Sannsynlighet vurderes
– Letthet, motivasjon,
kapasitet, frekvens
- Eksempler: [Bok om
Nasjonalt risiko
2014](#) (s205)



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.

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

- 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>

Krav til informationsikkerhet, 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

Spionerte på Telenor-sjefer, tømte all e-post og datafiler

Flere sjefer i Telenor ble utsatt for omfattende dataspionasje. Datamaskinene ble tømte for all data. Fredag ble det registrert usvanlig internett-trafikk fra Kripos.

Per Anders Johansen
Publisert: 17. mar. 2013 07:20 Oppdatert: 17. mar. 2013 07:20

165 likes, 4 anbefal

- Dette er første gang Telenor offentliggjør klart eksempel på målrettet industriespionasje mot Telenor. Rune Dyrbye, leder for Industriespionasje mot Telenor ble registrert usvanlig internett-trafikk fra Kripos.

Aftenposten

Problemer med innlogging i Altinn er løst

580.000 brukere skal kunne sjekke selvangivelsen sin i dag.

Oystein Aldridge
Publisert: 19. mar. 2013 09:23 Oppdatert: 19. mar. 2013 10:32

0 likes, 0 anbefal

Tirsdag får skattebetalere som aktivt har e-brukere, tilgang til selvangivelsen sin i dag. I morgentimene tirsdag opplevde enkelte brukere problemer med å logge seg inn på Altinn. Problemet gikk ut på at brukere ikke fikk meldinger om de trenger for å få tilgang til selvangivelsen sin i dag.

- Systemet ble friskmeldt 10 på 10.

Aftenposten

Nasjonale sikkerhetsmyndighet

Sikkerhetsbloggen

Aktuelt

- Mediebrief fra NSM
- Nytt fra NSM
- NSM i media

Nasjonale

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

**** Feilen rettet opp onsdag morgen**
**** Altinn-direktør: Sterkt beklagelig**

VG Nett 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 Kippemes](#)

15 tweets, 0 +1, 54 anbefal

Hovedsaken nå
[Les hele saken](#)

(VG Nett) En teknisk feil sørget for at flere personer tirsdag ble logget på som en helt annen.

VG fikk tirsdag kveld det første tipset fra en bruker som hadde logget seg på med BankID, og kom inn på en for ham helt ukjent person.

- Jeg har ingen kjennskap til ham. Det så ut som jeg hadde fri tilgang til informasjonen hans, men jeg valgte å ikke snoke for mye, forteller mannen - som tok en printscreen av det som møtte ham hos Altinn.

- Jeg logget ut og inn igjen, og var da på min egen profil igjen, forteller han

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!

Finnsøk: altinn

VG

Informasjonssikkerhet i media

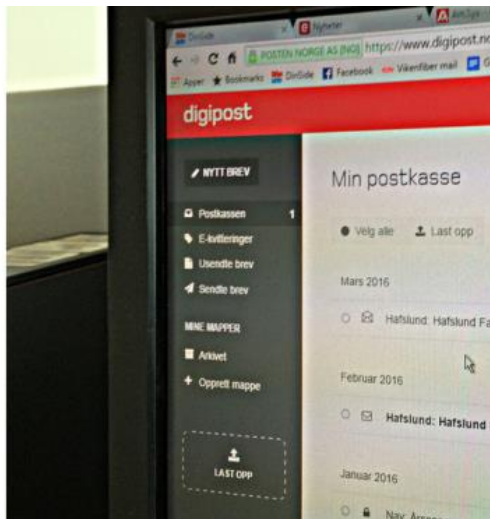
Norge Siste nytt Dokumentar Klima

Ny rapport: All kommunene

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



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



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

- Digipost er sikrere

24

Det mener sikkerhetsrådgiveren 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



Tirsdag offentliggjorde Helsetilsynet i Norge etter at samarbeidsreformer

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.

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 artikel 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 **integreert 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
 - Egnede 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 kryptorum

... Dører til kryptorum 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 kryptorum. 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?