

# Noen historier fra arbeidet med informasjonssikkerhet


Øyvind Grinde, NIFS, 29. november 2023

HELSE  SØR-ØST

# Kryptografi




ETSI TS 100 289 V1.2.1 (2014-03)




Technical Specification

Digital Video Broadcasting (DVB):  
Support for use of the DVB Scrambling Algorithm version 3  
within digital broadcasting systems



OPERATING EUROVISION




Digital Video  
Broadcasting



CRYSTALS  
Cryptographic Suite for Algebraic Lattices

CRYSTALS Kyber Dilithium



# Dataangrep

**HackCon**

0 dager igjen

Forside Om HackCon Program HackCon#1 Påmelding HackCon#1 Kontakt/Kontaktskjema

- + Om HackCon
- + Program HackCon#1
- + Påmelding HackCon#1
- + Administrativ informasjon
- + Konkurranser
- + Foredragsholder?
- + Om oss
- + Sponsorer
- + For media
- + Forum
- + Kontakt/Kontaktskjema
- + Driftsmeldinger

**HackCon#1**  
**Oslo den 8. og 9. februar 2006**

Konferansen ble fulltegnet den 5/1/2006.

Det er nå opprettet venteliste.  
Bruk påmeldingsskjema til å melde deg på for å komme med på ventelisten.

Husk å lese driftsmeldinger.

HackCon#1 arrangeres i Oslo 8. og 9. februar 2006

Antall plasser er begrenset  
Fulltegning pr. 22/12: 100%

Siste 20 reserveplasser:  
Fulltegning pr 5/1: 100%

Vi støtter nettsidene

.....  
[www.nettguiden.info](http://www.nettguiden.info)  
Bli med på å lage Norges største erfaringsdatabase om produkter og firma i Norge.

.....  
[www.blisikker.net](http://www.blisikker.net)  
For foreldre og barn

For åpen, fri og objektiv informasjonsflyt  
Better safe than sorry  
Denne siden ble generert av publiseringssystemet Pub:IT.Net på 0,3478 sekunder

Microsoft er en av plattformene som angripes av hackere. Utvikler/analytiker fra Microsoft Labs vil demonstrere hvordan man effektivt beskytter seg mot dette m.m.



Analysearbeidet etter dataangrepet mot Sykehuset Innlandet er avsluttet

Sykehuset Innlandet HF har i samarbeid med Sykehuspartner HF brukt store ressurser på kartlegging og analyse etter dataangrepet mot Sykehuset Innlandet den 22. august.

Publisert 15.09.2020 / Sist oppdatert 15.09.2020

## Kripos: Flere personer i kriminelt nettverk pågrepet

En av hovedmennene i en organisert kriminell gruppering politiet mener sto bak angrepet mot Hydro i 2019, ble pågrepet i Ukraina i forrige uke. En armensk statsborger, mistenkt for å ha deltatt i samme kriminelle gruppe, ble i oktober overlevert til Norge og varetektsfengslet.

Publisert i dag kl. 09.08 | Av: Kripos | Nyhet



# Risikobasert tilnærming

— Det er et svært alvorlig sikkerhetsbrudd når uvedkommende får tilgang til noens personopplysninger. Dette skal ikke kunne skje, og Altinn forblir stengt til vi er helt trygge på at løsningen i Altinn er sikker, fastslår fungerende skattedirektør Sven Rune Greni.



## Altinn stengt etter skatteskandale

Personopplysningene til mann (36) blottlagt.



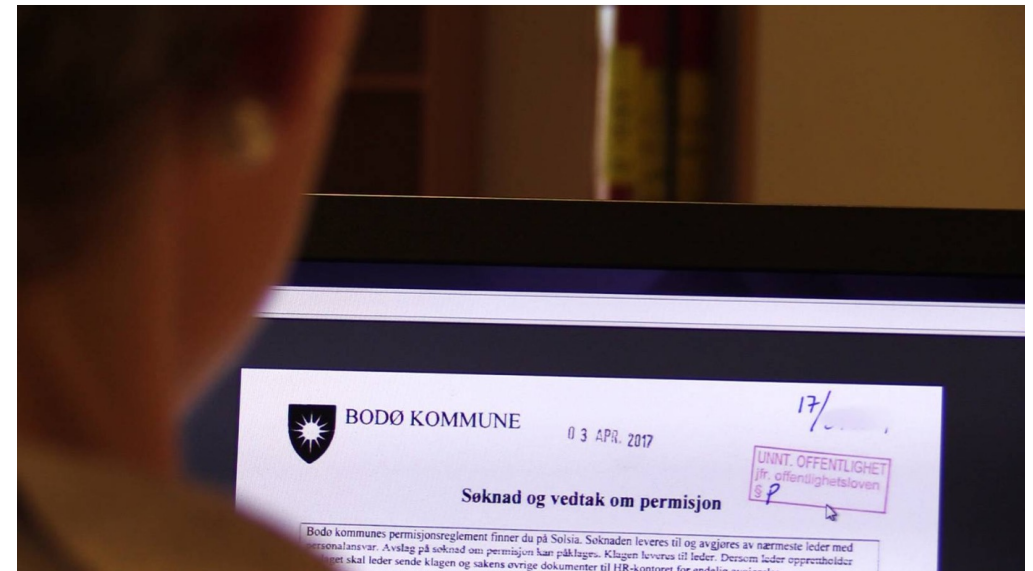
Logg på

Nordland

Nyhetscenter Valg 2023 Mobilvideo Snakk med oss TV Radio Tips oss!

## - Personopplysninger var ikke helt sikre før heller. De kunne dukke opp på ei søppelfylling

Det er umulig å sikre seg 100 prosent mot at sensitive opplysninger havner på avveie, ifølge Direktoratet for forvaltning og IKT. – Det må vi bare leve med, sier seksjonssjef.



Ved å endre dokumentnummeret i adressefeltet i Bodø kommunes elektroniske postjou... Vis mer



Kriterier for vurdering og  
aksept av risiko innen  
informasjonssikkerhet

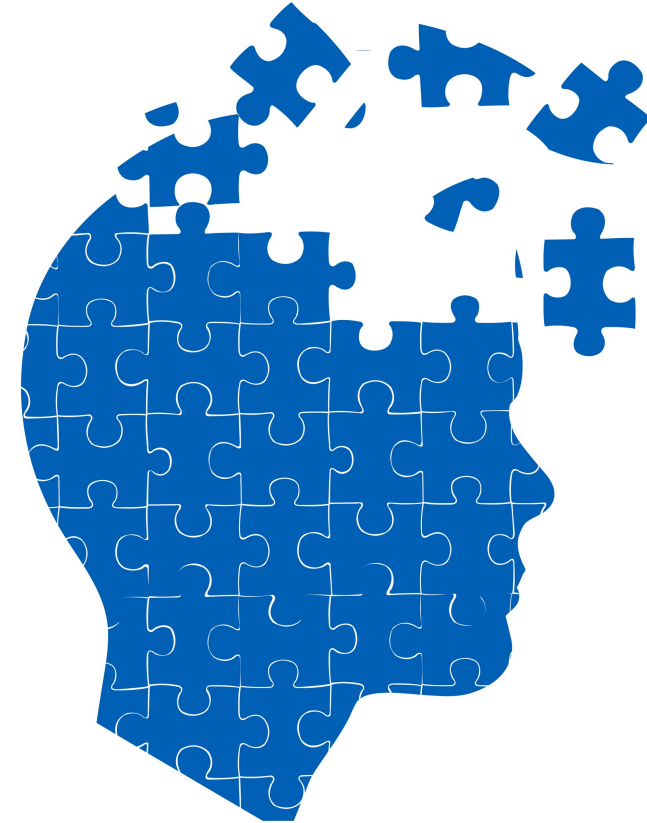
- Beslutninger om hvorvidt en risiko er akseptabel, skal tas av risikoeier.
- Aksept av høyere risiko krever beslutning på høyere ledelsesnivå.
- Der foreløpige analyser tyder på høy risiko skal både risikovurderingene og vurdering av mulig risikohåndtering gjøres grundigere enn ved lav risiko.
- Dersom helseforetaket er kjent med hvordan risikoen er vurdert i andre foretak, skal vurderingen hensyntas i akseptvurderingen.

# Informasjonssikkerhetskultur og -kompetanse

Digital sikkerhetskultur måles årlig

Sikkerhetsnytt fra Sykehuspartner

Hoxhunt – opplæring for å oppdage falske e-poster



Holdningen til digital sikkerhet er jevnt over ganske god i Helse Sør-Øst, selv om det er enkelte forbedringspunkter

# Oversikt over hvilke oppgaver og tjenester som utføres, og informasjonsbehandlingen i disse

## Trinn 1 - Identifisere oppgaver og informasjonstyper

Trinn 1 handler om å identifisere hvilke oppgaver og tjenester som utføres i enheten. Deretter må man identifisere informasjonstypene som behandles og relevante forhold knyttet til dem.

1 Identifiser oppgaver og informasjonstyper

2 Finn høyeste konsekvensnivå

3 Vurder trusler, farer og sårbarheter

Vi anbefaler å benytte «MAL Foranalyse trinn 1 - Oppgaver og informasjonstyper» i utførelsen av dette trinnet. Malen inneholder en oversikt over oppgaver som kan tilpasses virksomheten. Oppgavene og tjenestene bør dokumenteres i hvert sitt støtteskjema.

HELSE SØR-ØST

Få oversikt og prioritere – informasjonssikkerhet  
Foranalyse del 1 - Risikoeiere  
Identifisere arbeidsoppgaver og informasjonstyper

### Oversikt over arbeidsoppgaver og informasjonstyper

<b>Organisatorisk enhet:</b>	Informasjonssikkerhet
<b>Ansvarsområde:</b>	Informasjonssikkerhet
<b>Oppdateringer</b>	
<b>Dato</b>	<b>Deltakere</b>
21.10.2019	Øyvind Grinde
14.1.2021	Øyvind Grinde
20.11.2023	Øyvind Grinde

#### 1 Arbeidsoppgaver – kort oversikt

<b>Oppgave</b>
<b>Informasjonssikkerhet</b>
Regionalt informasjonssikkerhetsarbeid
Informasjonssikkerhetsarbeid i Helse Sør-Øst RHF

#### 2 Utdypninger - Arbeidsoppgaver, informasjonstyper mv.]

##### 2.1 Informasjonssikkerhetsarbeid

<b>Om arbeidsoppgaven og formålet</b>							
<b>Navn på arbeidsoppgave:</b>	Informasjonssikkerhetsarbeid   <b>Dato:</b> 20.11.2023						
<b>Formål med arbeidsoppgaven:</b>	Bidra til systematisk arbeid med informasjonssikkerhet i regionen og i Helse Sør-Øst RHF.						
<b>Kort beskrivelse av arbeidsoppgaven:</b>	Lede regionalt sikkerhetsfaglig råd (RSR). Lede interregionalt samarbeidsnåte for informasjonssikkerhet. Videreutvikle regionalt ledelsessystem for informasjonssikkerhet. Gi støtte og råd for informasjonssikkerhet. Kontrollere etterlevelse. Bidra til rapportering til eier og styret. Bidra til kravsetting av helseforetak.						
<b>Om informasjonsbehandling i oppgaven</b>							
<b>Informasjonstyper</b>	<b>Paragraf for potensiell taushetsplikt / unntak fra offentlighet</b>	<b>Spesielt obs mht. informasjonssikkerhet</b>	<b>Personopplysninger</b>	<b>Sjermingsverdig (S)</b>			
		<b>K</b>	<b>I</b>	<b>T</b>	<b>Ja/?</b>	<b>Særlig kategori?</b>	<b>Ja/?</b>
Agenda, Saksgrunnlag, presentasjoner og møtereferat for regionalt sikkerhetsfaglig råd.	Offl. §§ 23, 24						
Nettside for Regionalt sikkerhetsfaglig råd (RSR)							
Dokumenter i ledelsessystemet for informasjonssikkerhet							
Informasjon om sårbarheter og hendelser	Offl. §§ 14, 21, 24	Ja			?	?	?

# Helhetlige anbefalinger

- eForvaltningsforskriften § 15
  - 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.
- Kommunal- og moderniseringsdepartementet har i brev datert 12. mars 2014 utpekt Difi til det organ som iht. forskriften skal gi anbefalinger på området.
  - Difi sine anbefalinger om standarder fremkommer i "Referanse katalog for IT-standarder i offentlig sektor" og på Difis veiledningssider for informasjonssikkerhet.

