IKT NORGE

ikt-norge.no

Hva kan vi lære av den siste tidens «outsourcings-skandaler»?

Torgeir Waterhouse
Direktør Internet & New Media
tw@ikt-norge.no
@tawaterhouse
http://www.linkedin.com/in/tawaterhouse

IKT NORGE

ikt-norge.no

eller fra GDPR til virkelighet?

Torgeir Waterhouse
Direktør Internet & New Media
tw@ikt-norge.no
@tawaterhouse
http://www.linkedin.com/in/tawaterhouse

spørsmålet er vel:

hvorfor
er vi her?

problemer?

opplagt!

men hvilke?

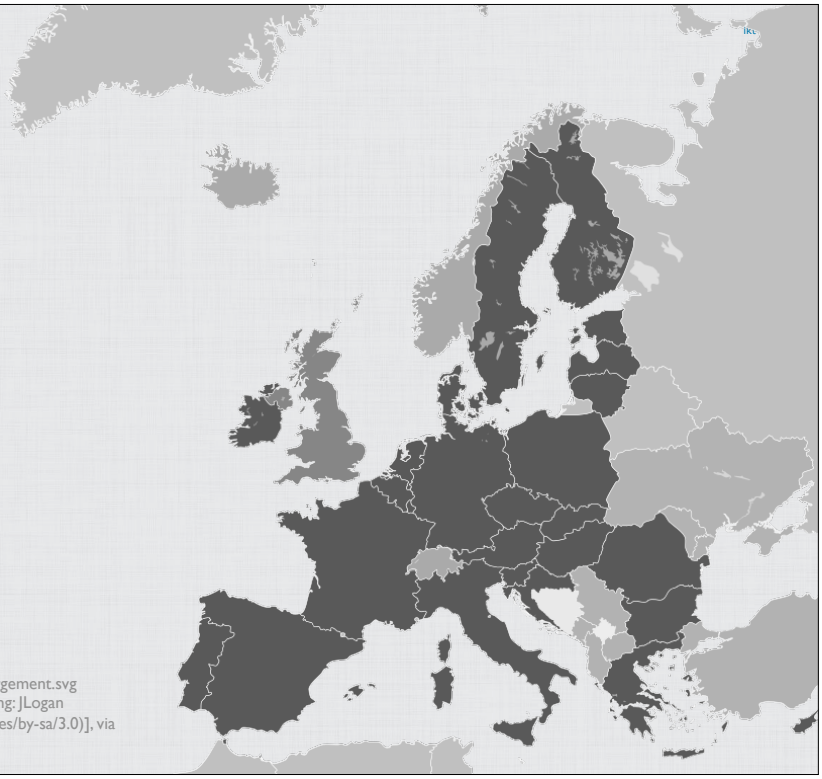
By BjørnN [Public domain], via Wikimedia Commons
https://commons.wikimedia.org/wiki/File%3AStamveier_Norge.svg

IKT NORGE IT-næringens interesseorganisasjon

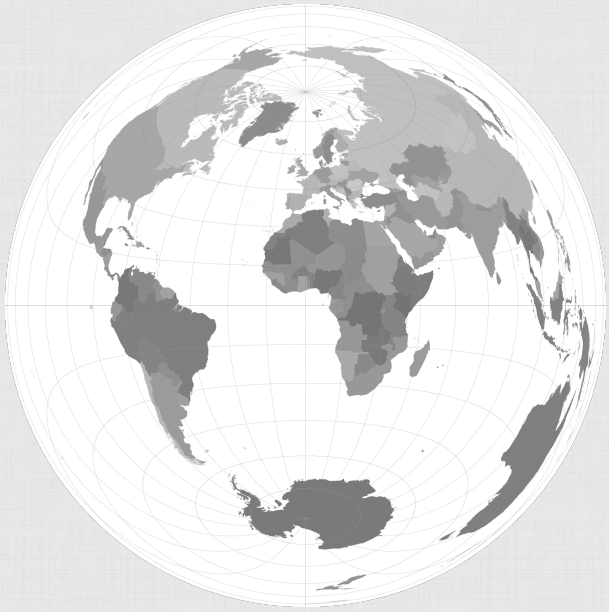
ikt-norge.no

https://commons.wikimedia.org/wiki/File%3ANorden_satellite.jpg
By Koyos (Own work by uploader, made with NASA World Wind.) [Public domain], via Wikimedia Commons

IKT NORGE IT-næringens interesseorganisasjon



https://commons.wikimedia.org/wiki/File%3AFurther_European_Union_Enlargement.svg
By Blank map of Europe.svg: maix¿? Further European Union Enlargement2.png: JLogan
Derivative work: JCRules [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons



https://commons.wikimedia.org/wiki/File%3AWorld_borders_lamb_azi.png
By Koenb at Dutch Wikipedia (Original text: productie van de afbeelding uit het .shp-bestand: Koenb) [Public domain], via Wikimedia Commons

Privacy Shield Framework

Hva kan vi* lære av den siste tidens «outsourcings-skandaler»?

Torgeir Waterhouse
Direktør Internet & New Media
tw@ikt-norge.no
@tawaterhouse
http://www.linkedin.com/in/tawaterhouse

*og hvem er vi?

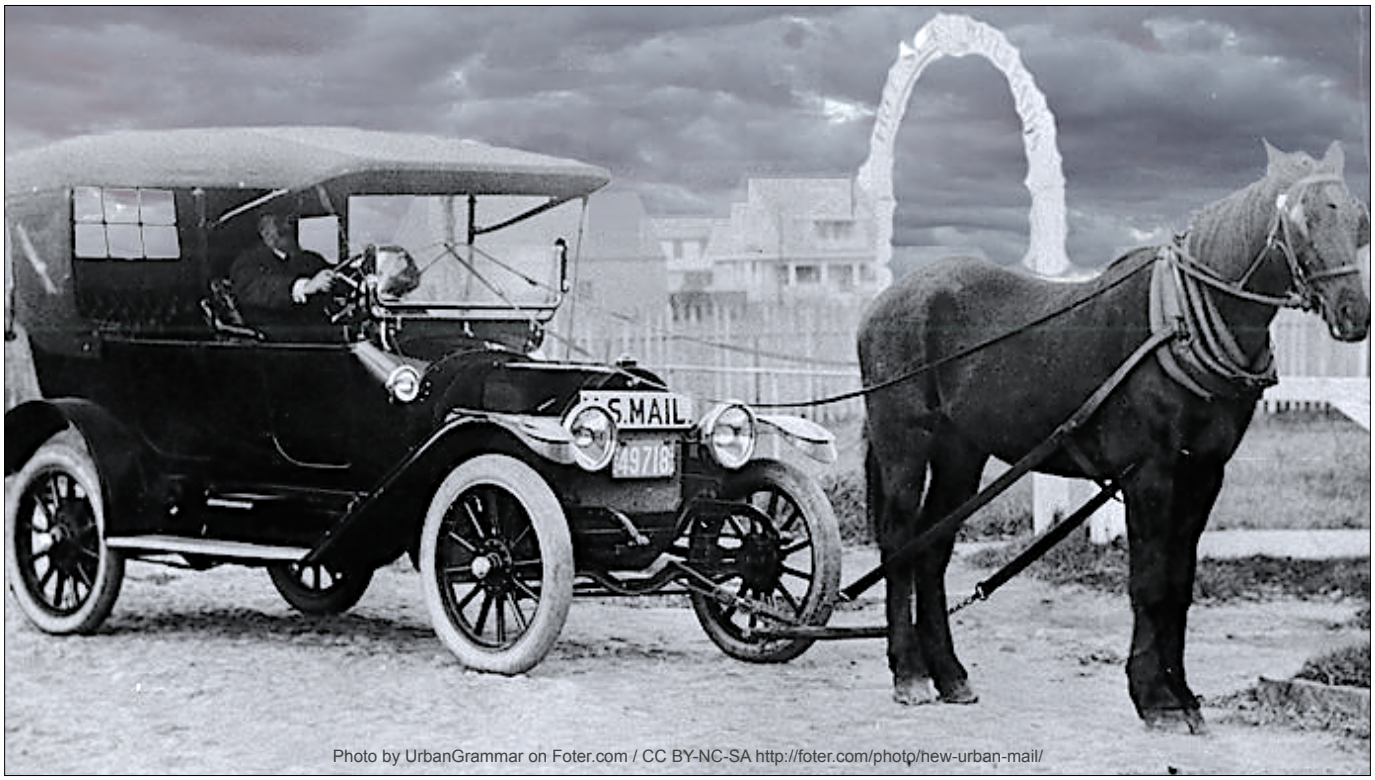


Photo by UrbanGrammar on Foter.com / CC BY-NC-SA http://foter.com/photo/new-urban-mail/

kompetanse vs vurderinger?

kan vi lære?

ledelse vs fag?

kan vi lære?

regler vs handling?

kan vi lære?

avtale vs handling?

kan vi lære?

backup vs restore?

kan vi lære?

diskusjonen vi har vs bør ha?

kan vi lære?

fagforeninger vs agenda?

kan vi lære?

outsourcing vs at home?

kan vi lære?

rett kompetanse vs nok kompetanse?

kan vi lære?

tolkning:

er antagelig ikke noe i veien for at sykehusene setter ut oppdrag slik de ønsker, men det må gjøres riktig, og vi må forstå hvordan risikoene varierer

kan vi lære?

mediedekning vs agenda?

kan vi lære?

"tilgang til 2.8 millioner nordmenns helseopplysninger"

NRK Dagsnytt 07.12.17

vs hvis vi leter lenge, virkelig lenge?

> Gjennom år har IT-sikkerheten i landets største helseforetak vært elendig uten at noen har tatt grep, viser rapporter og styredokumenter som NRK har gjennomgått.

https://www.nrk.no/norge/helse-sor-ost_-betrodde-medarbeidere-holdt-tilbake-informasjon-om-risikoen-ved-outsourcing-1.13577233

forstår vi* den tekniske gjelden?

*og hvem er vi?

forstår vi* outsourcing?

hva outsourcing egentlig er?

*og hvem er vi?

forstår vi* teknologien?

*og hvem er vi?

forstår vi* konsekvensene av teknologien?

*og hvem er vi?

forstår vi* brukerene?

*og hvem er vi?

“

technology is easy, people and their feelings are hard

”

Patient 86

fjernkontroll

vs åpningstider/tilgjengelighet

vs dataintegritet

vs kompetanse

vs kapasitet som vi bruker til hva?

vs **økonomi** som vi bruker til hva?

vs **mer**, mye mer

“

ikke har etterlevd sitt sikkerhetsansvar, ved å unnlate å gjennomføre og dokumentere sikkerhetsanalyser og sikkerhetstiltak og ved bevisst å ha avveket fra sikkerhetslovgivningen

”

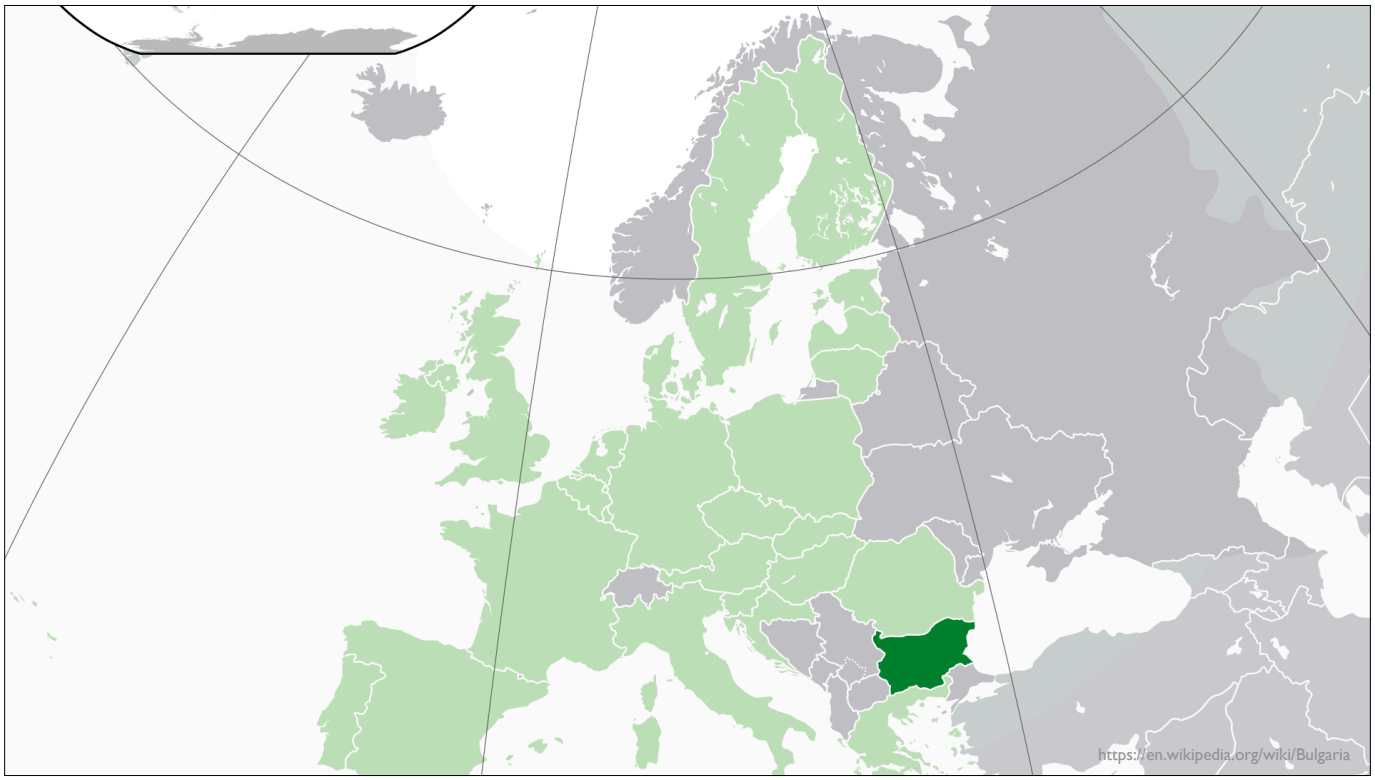
HELHETLIG IKT-RISIKOBILDE 2017 015: https://nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf

European Union

Council of Europe

OSCE

UN Security Council



NATO

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk

Art. 32 GDPR - Security of processing

fordi Bulgaria og Norge er forskjellige!

heller ikke sikkerhetsloven gir automagi,

men påvirker bla hvem som kan bruke data

Mangelfulle rutiner eller svak oppfølging sikkerhet følges ikke opp systematisk.

HELHETLIG IKT-RISIKOBILDE 2017 015: https://nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf

Hovedfunn fra NSMs tilsyn med virksomheters styring av sikkerhetsarbeidet i virksomheter underlagt sikkerhetsloven:

- Mangelfulle rutiner eller svak oppfølging – sikkerhet følges ikke opp systematisk.
- Implementering av de fire store hovedtiltakene innen sikkerhetsstyring – verdivurdering, risikoanalyser, internrevisjon og ledelsesevaluering – er krevende for mange virksomheter.
- Virksomhetene ville ha avdekket de fleste avvik som vi avdekker under tilsyn hvis de hadde gjennomført gode interne sikkerhetsrevisjoner.
- Manglende tilgangsstyring og soneinndeling – i datasystemer og fysisk sikring av lokaler.
- En del virksomheter mangler grunnleggende sikkerhetsfaglig kompetanse eller benytter ikke tilgjengelig sikkerhetsfaglig kompetanse systematisk og i tilstrekkelig grad.
- Mange virksomheter har ikke kompetanseplaner eller annen oversikt over den sikkerhetsfaglige kompetansen i virksomheten.
- Få virksomheter synes å registrere og rapportere sikkerhetstruende hendelser, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.
- Oppfølgingstilsyn viser at virksomheter iverksetter tiltak på bakgrunn av påviste mangler. Dette er positivt.

Få virksomheter synes å registrere og rapportere sikkerhetstruende hendelser, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.

HELHETLIG IKT-RISIKOBILDE 2017 015: https://nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf

Hovedfunn fra NSMs tilsyn med virksomheters styring av sikkerhetsarbeidet i virksomheter underlagt sikkerhetsloven:

- Mangelfulle rutiner eller svak oppfølging – sikkerhet følges ikke opp systematisk.
- Implementering av de fire store hovedtiltakene innen sikkerhetsstyring – verdivurdering, risikoanalyser, internrevisjon og ledelsesevaluering – er krevende for mange virksomheter.
- Virksomhetene ville ha avdekket de fleste avvik som vi avdekker under tilsyn hvis de hadde gjennomført gode interne sikkerhetsrevisjoner.
- Manglende tilgangsstyring og soneinndeling – i datasystemer og fysisk sikring av lokaler.
- En del virksomheter mangler grunnleggende sikkerhetsfaglig kompetanse eller benytter ikke tilgjengelig sikkerhetsfaglig kompetanse systematisk og i tilstrekkelig grad.
- Mange virksomheter har ikke kompetanseplaner eller annen oversikt over den sikkerhetsfaglige kompetansen i virksomheten.
- Få virksomheter synes å registrere og rapportere sikkerhetstruende hendelser, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.
- Oppfølgingstilsyn viser at virksomheter iverksetter tiltak på bakgrunn av påviste mangler. Dette er positivt.

hva da sikkerhet?

sikre nettverk(?)

nasjonal sikkerhet?

informasjonssikkerhet?

leveransesikkerhet?

sikker tilgang til data?

sikkert ytre skall?

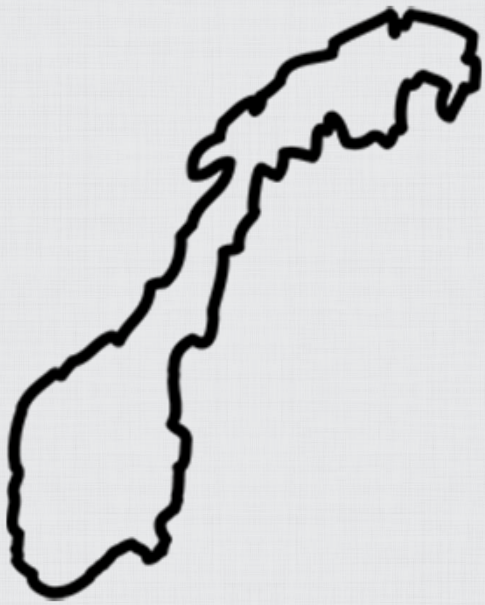
sikkerhet in-house?

sikker beredskap?

sikre brukere?

sikkerhetskunnskap?

etc...



Halve befolkningen ligger i databasen til Min idrett. Nå stenges søk etter avsløring

10

IT-eksperter bekymret for sikkerheten rundt stortingsvalget

NTB

OPPDATERT: 28.AUG.2017 13:44 | PUBLISERT: 28.AUG.2017 13:44

Illustrasjonsfoto: Terje Pedersen / NTB scanpix

Mange av stemmene ved årets stortingsvalg blir telt opp av datamaskiner tilkoblet internett. Eksperter er bekymret for IT-sikkerheten.

https://www.aftenposten.no/norge/politikk/i/g8v9J/IT-eksperter-bekymret-for-sikkerheten-rundt-stortingsvalget

Nei, Frode Thuen, det er ikke «et sunt prinsipp» at partneren skal ha tilgang til telefonen | Torgeir Waterhouse

TORGEIR WATERHOUSE, DIREKTØR IKT NORGE

OPPDATERT: 13.OKT.2017 13:09 | PUBLISERT: 13.OKT.2017 12:19

DEBATT

Frode Thuen og A-magasinet ber tjene arbeidslingen, og heller skrive noe om hvorfor det ikke er en god idé for mange å dele tilganger, oppfordrer Torgeir Waterhouse.
FOTO: Silo B. Hansen // Ashild Irgens // privat

Bare spør offer for overvåkende og voldelige partnere.

https://www.aftenposten.no/meninger/debatt/i/kAqeX/Nei_-Frode-Thuen_-det-er-ikke-et-sunt-prinsipp-at-partneren-skal-ha-tilgang-til-telefonen--Torgeir-Waterhouse

https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

“

Sårbarheter finnes i nær sagt alle virksomheter, systemer og infrastrukturer, både av teknisk, organisatorisk og menneskelig art.

”

HELHETLIG IKT-RISIKOBILDE 2017 015: https://nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf

“

NSM ser et økende gap mellom behov for og tilgjengelighet av sikkerhetskompetanse, noe som utgjør en nasjonal sårbarhet.

”

https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

> Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan bøte på denne utfordringen og bidra til bedre sikring av virksomheters nettverk og verdier.

https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

> Tjenesteutsetting, inkludert skytjenester, krever gode risikovurderinger og høy bestillerkompetanse innenfor en rekke områder.

https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

> NSM anbefaler likevel bruk av denne typen tjenester, forutsatt at det gjøres en grundig risikovurdering

https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

sikkerhet: data

sikkerhet: database

sikkerhet: fagsystem

sikkerhet: hardware

sikkerhet: nettverk

sikkerhet: drift

Prediction: Through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

http://www.networkworld.com/article/3088084/security/gartner-s-top-10-security-predictions.html

Prediction: By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.

http://www.networkworld.com/article/3088084/security/gartner-s-top-10-security-predictions.html

sikkerhet: bruk

“

the typical firm has on the order of 15 to 22 times more cloud applications running in the workplace than have been authorized by the IT department.

”

http://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html

når diskuterer vi: følelser?

når diskuterer vi: politikk?

når diskuterer vi: patriotisme?

når diskuterer vi: arbeidsplasser?

når diskuterer vi: kommunikasjon?

når diskuterer vi: kvalitet?

når diskuterer vi: sikkerhet?

når diskuterer vi: personlige agendaer?

når diskuterer vi: liv og helse?

er å drifte selv lik drift uten eksterne?

er anskaffelse lik-ish om drift er intern eller ekstern?

og hva med utredning, prosjekt, opplæring, drift, oppfølging, kontroll, videre utvikling, etc

også om egne ansatte gjør jobben in-house

aldri helt sikker, alltid en risikoprofil

nesten uansett model:

er det samme(ish) type risiko & samme(ish) type behov for tiltak?

Hva kan vi* lære av den siste tidens «outsourcings-skandaler»?

*og hvem er vi?

ledelsesansvar & vurderinger på rett nivå

hvilken ledelse & hvilket org.ledd*

*feks helseregion vs sykehus

dokumentasjon av alle elementer

oppfølging av alle elementer

kontroll på alle elementer

privacy by design

security by design

påstand:

dette er vi* ikke gode nok på, hverken innenfor eller utfor det norske huset,
selvfølgelig med noen (altfor få) unntak

Torgeir Waterhouse
Direktør internett og nye medier
tw@ikt-norge.no
@tawaterhouse
http://www.linkedin.com/in/tawaterhouse

*og hvem er vi?