
UNIT
Direktoratet
for IKT og fellestjenester
i høyere utdanning
og forskning

Kjøreplan

- To hovedområder:

    1) Resultatene fra Units 2019-kartlegging av arbeidet med informasjonssikkerhet (og personvern) i universitets- og høgskolesektoren

    2) Oversikt over noen viktige informasjonssikkerhetsspørsmål på økonomiområdet

- NB: Units 2019-kartlegging hadde ikke spesielt fokus på informasjonssikkerhet i økonomisystemer

Kartlegging – informasjonssikkerhet og personvern

- Årlig kartlegging som gjennomføres av Unit
- Omfatter alle statlige universiteter og høgskoler, direktorater og AS-er (31 virksomheter)
- Inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern
- Rapport tilgjengelig på Unit sine hjemmesider (https://www.unit.no/sites/default/files/media/filer/2019/06/Tilstandsvurdering-av-informasjonssikkerhet-personvern-blant-de-statlig-eide-universitetene-og-hogskolene.pdf)

Det som skal beskyttes

- Omfattende, sammensatt og (til dels) uoversiktlig verdiportefølje
  - forskningsdata
  - forskningsresultater
  - undervisningsressurser
  - administrative data, inkludert økonomidata
  - dataressurser (datanettverk, systemer og tjenester)
  - økonomiske midler
- Personopplysninger i forskning, undervisning og administrasjon

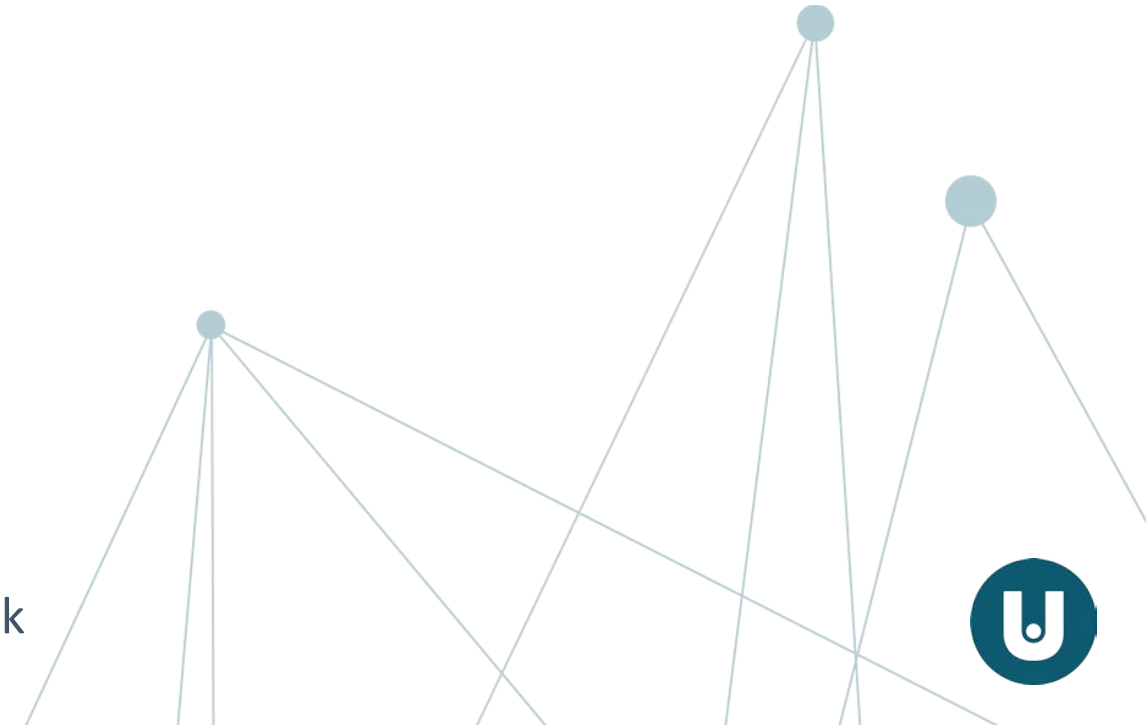
Informasjonssikkerhetshendelser, 2017-18

- Mange mindre, få store hendelser

- Det vanlige
  - nettfiske («alle og enhver»)
  - målrettet nettfiske (persontilpasset)
  - løsepengevirus
  - ID-tyveri (brukerkontoer på avveie)
  - brudd på personopplysningssikkerheten

- Det (litt) spesielle
  - misbruk av dataressurser
  - kunnskapstyveri/spionasje

- Mistanke om underrapportering av hendelser og avvik



Skadevirkningene

- Vanskelig å anslå skadevirkningene i kroner og øre

- Følgende typer skadevirkninger ble rapportert:
  - ekstraarbeid
  - omdømmetap
  - kunnskapslekkasje
  - personvernkrenkelser
  - økonomisk tap
  - tap påført andre virksomheter
  - intern «støy»

Hvorfor skjer ikke mer?

- Virksomhetene rapporterte om viktige initiativ/tiltak i for å styrke informasjonssikkerheten:
  - innføring/drift av ledelsessystemer/internkontroll (10 av 21 virksomheter)
  - gjennomført bevisstgjørings- eller opplæringstiltak (alle virksomheter)
  - økt bruk av risikovurderinger (18 av 21 virksomheter)
  - høyt fokus innenfor på visse forsknings- eller utdanningsområder (alle virksomheter)
  - IT-avdelingenes aktive rolle (alle virksomheter)
- Toppledelsen og styrene mer med

Hvorfor skjer ikke mindre?

- Virksomhetene rapporterte om viktige utfordringer i arbeidet med informasjonssikkerhet

- De viktigste utfordringene:

  - manglende personalressurser og kapasitet (19 av 21 virksomheter)
  - mangelfull informasjonssikkerhetskompetanse (19 av 21 virksomheter)
  - manglende innføring av ledelsessystemer (11 av 21 virksomheter)
  - teknisk og organisatorisk kompleksitet (alle virksomheter)
  - manglende kontinuitetsplaner (20 av 21 virksomheter)

Økonomiregelverket i staten

- Bestemmelsene punkt 2.4 («Internkontroll»)
  - «rutiner for behandling og lagring av vesentlig informasjon som sikrer konfidensialitet, integritet og tilgjengelighet»

- Bestemmelsene punkt 2.6 («Organisering av økonomioppgaver»)
  - krav til «tilstrekkelig datasikkerhet» ved tjenesteutsetting av økonomioppgaver eller økonomisystemer

- Bestemmelsene punkt 4.3.6 («Sikkerhet i økonomisystemet»)
  - bl.a. krav til tilgangsstyring og aktivitetslogging

- Bestemmelsene punkt 4.4.9.3 («Sikkerhetskopi»)
  - bl.a. krav til oppbevaring og testing av sikkerhetskopier av elektronisk regnskapsmateriale

Trusler og hendelser som gjelder økonomisystemer

- Hovedtrussel – kriminelle grupper på internettet
  - motivasjon – økonomisk vinning

- Hendelser som økonomimedarbeidere/-ledere kan utsettes for
  - direktørsvindel
  - leverandørsvindel
  - brukerkontoer på avveie
  - løsepengevirus
  - interne feil eller svakheter

- Ikke rapporter om store skadevirkninger på økonomiområdet som følge av slike hendelser

Særlig relevante risikoområder

- Behov for fortsatt fokus på
  - tilgangsstyring og rettigheter, spesielt BDM
  - håndtering av brukernavn og passord
  - kontroll med utbetalinger (falske fakturaer)
  - tydelige krav til informasjonssikkerhet i avtaler med eksterne systemleverandører
  - kontroll med at systemleverandører overholder avtalte sikkerhetskrav

Generelle anbefalinger – institusjonsnivået

- Prioritere arbeidet sterkere
  - personell, kompetanse og samordning
- Innføre og praktisere ledelsessystemer
  - spesielt på enhetsnivå
- Ha noe bedre oversikt over informasjonsverdier
- Ha fokus på kontinuitet

Generelle anbefalinger – nasjonalt nivå

- Det bør defineres tydelige sektormål
- Det bør fokuseres på forskning og undervisning
- Det bør etableres en konsulent- og rådgivingstjeneste
- Det bør stilles tydelige krav ved utvikling eller anskaffelser av fellesløsninger