Informationssäkerhet – krav, behov och verklighet

Fia Ewald CONSULTING AB

Krav

Två perspektiv

- Externa krav
- Den egna organisationen (behov)

Värt att notera:
Myndigheten är skyldig att upprätthålla ett grundläggande skydd för sina ”handlingar”

Externa krav

- MSBFS 2016:1
- MSBFS 2016:2
- Dataskyddsförordningen
- Totalförsvar
- E-förvaltning

MSBFS 2016:1

- Ett infört LIS – organisatorisk styrning av informationssäkerhet
- Ansvar –befogenheter
- Säkerhetskultur
- Riskanalys
- Informationsklassning – skyddsåtgärder
- Incident- och kontinuitetshantering
- Outsourcing/e-förvaltning
- Uppföljning

MSBFS 2016:1

- 11 § Myndigheten ska ha rutiner för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott. **Förhållanden som kan uppstå i samband med fredstida kriser och under höjd beredskap ska beaktas.**

MSBFS 2016:2

- … ska rapportera it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten levererar till en annan organisation…
- …rapportera en it-incident senast 24 timmar efter det att myndigheten upptäckt den rapporteringspliktiga incidenten…
- I det fall en myndighet har polisanmält en it-incident behöver myndigheten inte lämna en rapport enligt 6 § utan endast en kopia på polisanmälan.

MSBFS 2016:2

”De rapporteringspliktiga it-incidenterna kan utgöras av kategorierna

1. störning i mjuk- eller hårdvara,
2. störning i driftmiljö,
3. informationsförlust eller informationsläckage,
4. informationsförvanskning,
5. hindrad tillgång till information,
6. säkerhetsbrist i en produkt,
7. angrepp,
8. handhavandefel,
9. oönskad eller oplanerad störning i kritisk infrastruktur, eller
10. annan plötslig oförutsedd händelse som lett till skada. ”

Dataskyddsförordningen

- Förordningen börjar gälla direkt som svensk lag 25 maj 2018 och ersätter PUL, gäller både myndigheter och företag
- Avsikten är att stärka individens rätt till integritet
- Krav på att vid dataintrång eller om ni på något annat sätt tappa kontrollen över personuppgifter så måste ni informera både de personer som uppgifterna gäller och Datainspektionen, om incidenten är allvarlig
- Hantering av personuppgifter som kan medföra stora integritetsrisker - först göra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (eventuellt inkalla DI)
- De särskilda regler om personuppgiftsbehandling som finns idag för olika svenska myndigheter utreds nu av dataskyddsutredningen
- Undantaget för ostrukturerad information (missbruksregeln) finns inte kvar utan bedömningen måste göras i den generella riskhanteringen
- Det kan bli böter….

Dataskyddsförordningen – individens rättigheter

- få tillgång till sina personuppgifter
- få felaktiga personuppgifter rättade
- få sina personuppgifter raderade
- invända mot att personuppgifterna används för direktmarknadsföring
- invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- flytta personuppgifterna (dataportabilitet)

Dataskyddsförordningen i ett informationssäkerhetsperspektiv

- Privacy-by-design
- God spårbarhet en förutsättning
- Incidenthantering och -rapportering
- Ordning och reda-frågor – kontroll över informationen
- Tydlig ändamålsdefinition
- Algoritmer och rätten att få uppgifter raderade…
- Portabilitet
- Internationella samarbeten?

(bättre information till de registrerade)

Totalförsvaret

- Planering inledd
- Statliga myndigheter ska kunna
  - Redan i fredstid ha förmåga att stå emot olika former av öppna och dolda påtryckningar
  - Öka sin förmåga att identifiera och möta underrättelseverksamhet, cyberattacker och informationsoperationer mot landet
  - Öka sin förmåga att motstå väpnat angrepp

E-förvaltning - nationellt

- Svåröverblickbart på nationell nivå
- Infrastruktur och tjänster
- Ansvarsförhållanden
- Informationssäkerhet en nedprioriterad fråga?

E-förvaltning – den egna organisationen

- Inriktning och strategi
- Ansvarsförhållanden i egna tjänster och i andra relationer
- Cloud first?
- Informationssäkerhet i tjänster

Verklighet

Det kanske inte funkar så bra…

Tre bortförklaringar som inte håller

- Det saknas pengar
- It-utvecklingen går så snabbt att gapet blir större och större
- Ledningen förstår inte frågan

Behov

Behov

- Behov i organisationen
- Behov hos den som jobbar med informationssäkerhet

Behov i organisationen

- Snabbt förändrad informationshantering
- Effektivitet och kvalitet
- Verksamhetsanpassad informationssäkerhet
- Organisatorisk styrning

Behov hos den som jobbar med informationssäkerhet

- Långsiktigt mandat
- Tydligt ansvar
- Resurser
- Kompetens och kunskap
- Kommunikativ förmåga
- Verksamhetsintegrering

Workshop: Det som inte finns i verksamhetsplanen finns inte

Uppgift 1

- Vad vill jag ha med i verksamhetsplanen?
- Hur får jag med det?

Uppgift 2

- Vad är gemensamma behov kring LIS inom SUSEC?
- Hur kan vi konkret och långsiktigt samarbeta kring dem?

Uppgift 3

- Vad innebär totalförsvar för lärosätena?
- Hur planerar vi för detta inom informationssäkerhetsområdet?

Uppgift 4

- Vad innebär dataskyddsförordningen för lärosätena?
- Hur planerar vi för detta inom informationssäkerhetsområdet?

Kontakt

fia@fiaewald.se

www.fiaewald.se

0705-741431

Fia Ewald CONSULTING AB