179.

RIKSREVISIONEN

Datum: 2023-06-09
Ange avdelning

Minnesanteckningar intervju MSB

Medverkande

- MSB: enhetschef
- RiR: Sara, Josefine, Ludvig

Plats: Digitalt

1. **Status NIS 2? Kommer forskning ingå?**
   MSB tycker att forskningen ska vara med. Ska det täcka public administration gäller det även för lärosäten. NIS 2 har till skillnad från NIS 1 fokus på framtida ekonomisk säkerhet. Där är forskning och innovation helt centralt.

   Det pågår en utredning just nu som ska redovisa slutsatser i februari nästa år. Sen ska regeringen hantera detta. Sen är implementeringsperioden klar 18 oktober 2024. Kommissionen kommer inleda tillsynsärenden mot medlemsstater tre månader efter implementeringsperioden, om man inte implementerat fullt ut, vilket Sverige sannolikt inte kommer ha gjort.

   Det är mycket som är oklart så det kommer antagligen innebära stora förseningar. FRA ska samordna i egenskap av att hålla i Centret för cybersäkerhet.

2. **Senaste Infosäkkollen innehåller också it-säk. Berätta om det.**
   Vi har propagerat för att Infosäkkollen ger en bra bild hur man jobbar processmässigt. Då blir det mkt kring riskanalys, ledningssystem etc. Men det har gjort att vi inte vet ngt från Infosäkkollen om vilka faktiska säkerhetsåtgärder när det gäller IT-system som man har på plats. Vi har bara undersökt om man säkerställt att man har rätt strukturer på plats för att kunna implementera rätt tekniskt skydd m.m. Det har vi sagt länge och sett ett behov att inkludera även åtgärder.

   Den nya regeringen ville ha data inom ramen för nya nationell säkerhetsstrategi. MSB fick ett tilläggsuppdrag pga. nya regeringen ville ha underlag.

MSB har propagerat för att de ska kunna ge stöd även till privata aktörer, NIS-aktörer.

Det vi gör nu är en slags lightversion, och så ska vi till 2025 skapa en mer ordentlig undersökning av IT-säk i Infosäkkollen.

Vi har kunnat utveckla detta arbete tidigare utan uppdrag från regeringen, men problemet är då att MSB inte har ett skydd för att bli stämda. Eftersom man går in på en marknad där det finns konkurrenter som erbjuder liknande tjänster men som kostar.

3. **Vad för stöd gällande informationssäkerhet efterfrågas från lärosätena? Vad frågar de er om? Vet ni om de vänder sig med frågor om informationssäkerhet till andra aktörer än MSB?**
   Det behöver jag fråga rådgivningsstöd om i så fall. Känner inte till att vi får så mkt frågor alls. Återkommer.

4. **Vilka på lärosätena efterfrågar stöd? Vilka hör av sig till er?**
   Se svar ovan.

5. **Har ni något särskilt stöd till lärosätena eller är det samma stöd som till alla myndigheter? Är det en bra idé?**
   Självklart går det att anpassa metodstödet vi har för särskilda ändamål och aktörer. Tycker inte att det är problemet. En infosäksamordnare på universitet som ska genomföra infoklassning kommer behöva göra det i samarbete med institutionerna och de olika forskningslagen. På ett stort universitet kommer inte en person räcka till. Då blir det en resursfråga. Sen är det så att om infoklassning är kopplad till skyddsnivåer och säkerhetsåtgärder, och de skyddsåtgärderna innebär att det blir jobbigare att jobba, då finns det incitament för forskarna att inte delta i detta arbete. Och så rinner det ut i sanden. Det finns massa institutionella aspekter i det här som är det stora problemet. Jag förhåller mig mkt tveksam att det är i stödet som skon klämmer.

6. **En del lärosäten säger att föreskrifterna (MSBFS 2020:6, 2020:7 och 2020:8) inte är anpassade för lärosäten och inte går att följa. Delar ni denna uppfattning?**
   De har försökt få oss att ändra föreskrifterna eller undanta lärosätena från föreskrifterna. De har omfattats av föreskrifterna sen 2011. De har aldrig följt dem och de har byggt massa digitala system sen dess som inte är förenliga med föreskrifterna. Lärosätena har gjort det lätt för sig. Utveckling sker på ad hoc-basis, där forskarna vill bygga ngt nytt. Då bygger man ad hoc så det ska passa dagsaktuella forskningsfrågor. Sen

dyker det upp en infosäkare som påpekar att det finns regler, då blir det en diskussion med forskarna och ledningen, och forskarna tycker det är för jobbigt. De säger att man inte kan jobba om man måste följa alla dessa regler, och då får infosäk ta ett steg tillbaka. Vi har mkt lite förståelse för detta.

De har byggt systemen så det inte går att följa föreskrifterna. Men de hade inte behövt bygga systemen på de sätten från början.

IMY har samma problem med UoH som vill ha undantag.

Tror inte att det är själva metodstödet som är problemet.

Kan du konkretisera vad för typ av system det handlar om som inte är förenliga med förskrifterna?
Kan ta med frågan och ge exempel sen. Men t.ex. att man inte kan tänka sig att ha nätverkssegmentering. Mkt av de tekniska säkerhetsåtgärderna gör att det blir lika smidigt för data att flöda. Men det är poängen, att det ska vara lite svårare, t.ex. för skadlig kod att flöda. Det är kärnan i problematiken, de vill ha enkla lösningar. Men då blir det också enklare för skadlig kod t.ex., det är sådant de inte vill ta tag i, för då tar allt mkt längre tid.

7. **Vad kan lärosätena göra för en bättre efterlevnad av föreskrifterna?**
Verktyg som kan ha effekt – t.ex. NIS 2 om det kommer omfatta forskningen. Pga. tillsyn som kommer vara ganska skarp. Böter (upp till 10 milj Euro), möjlighet att avsätta chefer. De kommer inte lämnas ifred på samma sätt längre. Och då är det inte infosäkfolket utan UoH:s ledningar som kommer att få stå till svars.

Vad är vägen framåt iom att de gjort fel sen 2011?
Man får skilja på de olika föreskrifterna – man måste resurssätta arbetet, stötta. MSBFS2020:6 handlar om att ta itu med resurser och struktur. Nåt annat än 2020:7 och 2020:8. Men med de tekniska delarna i föreskrifterna... det kommer ju bli dyrt, och det är inte lämpligt för mig att svara på, MSB kan inte ta ansvar för att lärosätena satt upp system som inte är förenliga med lagkraven. Men när man bygger nya system så kan man se till att inte göra samma misstag igen. Om man i grunden har osäkra systemlösningar så kan man t.ex. jobba med förhållningsregler, normer, sätt att arbeta på som åtminstone reducerar risken för att det ska gå illa nu när det ser ut som det gör

Mycket av det som gör det osäkert är att samspelet mellan människa och system inte är bra.

Det är problematiskt som byråkrat att komma med alternativa råd än i enlighet med de uppdrag vi fått från regeringen.

Lärosäten säger ofta att de behöver väldigt olika lösningar för att forskningen är så olika – hur bemöter man det?
Man kan vända på det, vad är det isf som hindrar er från att bygga den här särlösningen men att göra det enligt gällande regler?

8. **Är det tekniskt och juridiskt möjligt att göra separata föreskrifter om informationssäkerhet för lärosätena?**
   Se resonemang ovan, tycker inte det behövs.

9. **Finns det saker utanför ert mandat som skulle behövas ändras för att förbättra efterlevnaden? [t.ex. regeringens styrning]**
   Skulle kunna införa krav på myndigheter att genomföra Infosäkkollen. Den sociala faktorn att inte vara sämst i klassen är också viktig och kan bidra till bättre efterlevnad

Övrigt

- Storskaliga forskningsdatabaser – där var resonemanget att bara stora lärosäten bör få hantera såna här. Där skulle man kunna kontra med att säga att bara lärosäten som har en påvisad god förmåga att hantera infosäk borde få använda såna. Man kan i samband med att såna här frågor kommer upp successivt inför saker som har en positiv incitamentsstruktur.
- Mitt intryck är att man kanske som forskare till och med väljer bort att komma till ett universitet om man har för mkt krav på infosäk. Lärosätena är medvetna om det och försöker hålla infosäk lite under radarn.
- Viktig poäng: Som forskare kan man ibland bli bedömd på hur lång tid det tog att genomföra ett forskningsprojekt. Om det tar lång tid att bygga upp infrastruktur och säkerhetslösningar för att kunna genomföra forskningen så kommer det ses negativt, att det tog lång tid och tog mycket resurser. Det finns jättestarka incitamentsstrukturer mot att inte beakta säkerhetslösningar, eftersom det tar tid och kostar. Här skulle finansiärerna kunna spela en roll genom att man som forskare kan söka pengar.
- Vill betona att när jag pratar om säkerhet så är det inte bara konfidentialitet, utan även t.ex. tillgänglighet
- De på lärosätena som påhälsat oss har ju ofta varit infosökpersoner. De kommer ofta inte hit med en personlig övertygelse om att de borde omfattas av ett annat regelverk. Men de har ofta stångat sig blodiga på sitt lärosäte. Successivt mals engagemanget ner och i slutändan landar man kanske i att föreskrifterna behöver lättas eller förändras för

lärosätena. Man har "förlorat" den interna kampen på lärosätet. Om det är någon som förtjänar kritik så är det ledningarna på lärosätena, inte de som jobbar med infosäk som försöker göra ett bra arbete.

- MSB spelade in formuleringar inför UoH regleringsbrev 2023, Infosäk-kollen nämns inte specifikt men det är hämtat från det.