UPPSALA UNIVERSITET

REMISSVAR

2024-05-28 Dnr UFV 2024/477

Box 256
75105 Uppsala

Handläggare
Tom Petersson

Telefon
0704250277

www.uu.se
tom.petersson@uu.se

Försvarsdepartementet
Fö2024/00496

Delbetänkandet Nya regler om cybersäkerhet SOU 2024:18

Ärendebeskrivning

Den 6 mars 2024 remitterade Försvarsdepartementet delbetänkandet Nya regler om cybersäkerhet SOU 2024:18.

Sammanfattning

Uppsala universitet stödjer ambitionerna om att öka ansträngningarna och kvalitén i lärosätenas säkerhetsarbete men anser att förslagen och konsekvenserna av förslagens genomförande inte är tillräckligt utredda. Förslagen kan också leda till en överimplementering av EU-lagstiftning som i förlängningen riskerar skada svensk forskning och utbildning.

Uppsala universitet lämnar förslag till förändringar och kompletteringar nedan.

Generella synpunkter

Uppsala universitet välkomnar de ambitioner om att öka kvalitén i säkerhetsarbetet i generell mening vid de svenska lärosätena som lagts fram under senare tid. Säkerhetsfrågorna är av största vikt i lärosätenas verksamhet och det finns ett behov av att höja medvetandet om de hot som riktas mot lärosätena likväl som att förbättra våra rutiner och vår handlingsberedskap.

Delbetänkandet Nya regler om cybersäkerhet och de förslag som lämnas däri, innehåller i vissa avseenden brister och reser påtagliga gränsdragnings- och tillämpningsproblem. Frågan om cybersäkerhet i den typ av komplexa organisationer som särskilt de breda lärosätena utgör, sätter ljuset på behovet av att ytterligare utreda den grundläggande frågan och att därefter anpassa formella regelverk, lagstiftning och förordningar efter de specifika förutsättningar som lärosätena verkar utifrån.

Uppsala universitet är väl medvetna om den generella och skarpa kritik som riktats mot lärosätenas säkerhetsarbete, av både Riksrevisionen och MSB. Vid Uppsala universitet har ambitionerna i och de resurser som avsätts till det kontinuerliga säkerhetsarbetet, bland annat som en följd av kritiken, höjts avsevärt.

Organisationsnummer:
202100-2932

UPPSALA UNIVERSITET

REMISSVAR

2024-05-28 Dnr UFV 2024/477

De förslag som läggs fram i delbetänkandet kommer medföra kraftigt ökade kostnader för lärosätenas säkerhetsarbete. Det är, givet den starkt pressade ekonomiska situation som Uppsala universitet i likhet med många andra lärosäten befinner sig i, anmärkningsvärt att inga som helst ekonomiska resurser ska tillföras sektorn för att uppfylla de nya reglerna om cybersäkerhet som föreslås. Oavsett dessa regelkrav så behöver lärosätena bedriva ett säkerhetsarbete som matchar hotbilden, vilket är kostsamt. Ett bättre sätt att stärka säkerheten vid lärosätena vore därför att tillföra nödvändiga kvalitetsresurser. Detaljregleringar riskerar att leda till att lärosätena inte väljer optimala åtgärder för att förbättra säkerheten, utan istället genomför åtgärder kopplade till detaljstyrningen.

Uppsala universitet anser att frågan om lärosätenas säkerhetsarbete, inklusive cybersäkerhet, måste hanteras på ett sammanhållet och koordinerat sätt för hela sektorn. De svenska lärosätena och deras verksamheter är i vissa avseenden inte jämförbara med statliga myndigheter i gemen. För ett kostnads- och verksamhetsmässigt effektivt säkerhetsarbete som ska fungera långsiktigt bör målsättningar och ambitioner inom säkerhetsområdet beredas i en dialog med lärosätena. SUHF är en resurs som i högre utsträckning borde utnyttjas för kunskaps- och erfarenhetsutbyte i detta sammanhang.

Uppsala universitet anser att delbetänkandet lägger alltför stort fokus på att bygga upp kontrollsystem och potentiella sanktioner, istället för att identifiera och uppmärksamma det allt mer påträngande behov som lärosätena har av stöd och dialog med de organisationer, till exempel MSB och Försvarshögskolan, som har expertkunskap inom området.

Specifika synpunkter

Förtydliga regelverken för klassificering och registrering respektive tillsynen av verksamhetsutövare som verkar inom flera sektorer (2 kap. 1 § resp. 6 kap 13 §)

Förslaget gör en åtskillnad mellan offentliga och enskilda verksamhetsutövare. Det framgår dock inte hur påverkan blir på de delar av verksamheten som inte har samma skyddsnivåer, t.ex. grundutbildning och studenters eget arbete inom program eller kurser, jämfört med högre forskning inom skyddsvärda områden som rymdteknik eller genteknik, eller jämfört med universitetets myndighetsutövning. Det finns ett antal lärosäten med examenstillstånd som är statliga myndigheter och som även bedriver verksamhet enligt bilaga 1 till NIS2-direktivet.

Av 6 kap. 13 § i förslaget till cybersäkerhetsförordning framgår att ”Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde i 8 §.”

UPPSALA UNIVERSITET

REMISSVAR

2024-05-28 Dnr UFV 2024/477

Stora forskningstunga universitet, som Uppsala universitet, verkar inom utbildningssektorn, inom offentlig förvaltning, hälso- och sjukvård (vårdgivare), forskning och utveckling avseende läkemedel, samt som digitala leverantörer, med digital infrastruktur (datacentraltjänster, molntjänster med mera) som erbjuds till andra myndigheter eller organisationer.

Tillsynsmyndigheter ska samarbeta, men ha tillsyn över respektive tillsynsområde. Det innebär, såvitt det kan bedömas, att verksamhetsutövare som bedriver verksamhet inom flera verksamhetsområden, till exempel stora lärosäten, kommer stå under tillsyn av flera olika myndigheter.

Uppsala universitet föreslår att regelverken kring tillsyn för verksamhetsutövare som verkar inom flera sektorer förtydligas, och att det tas särskild hänsyn till förutsättningarna för breda lärosäten.

Minska antalet tillsynsmyndigheter (2 kap. 2 §)

Förslaget anger i 2 kap 2 § att ”Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs.”

Anmälningarna ska innehålla känsliga uppgifter, både med avseende på IP-adressintervall och i vilka länder som verksamhet bedrivs. Verksamhet som bedrivs i olika länder kan för ett forskningsuniversitet innebära uppgifter om känslig forskning, forskningssamarbeten, dyrbar utrustning, med mera. Det är med andra ord uppgifter som behöver kunna anmälas på ett säkert sätt, till så få tillsynsmyndigheter som möjligt och med garantier om överförd sekretess både vad gäller inrapportering och lagring hos tillsynsmyndighet(-erna).

Aggregerade uppgifter från många verksamhetsutövare har dessutom potential att vara högst intressant information för angripare.

Uppsala universitet föreslår att antalet tillsynsmyndigheter som ska ta emot anmälningar hålls till ett minimum. Anmälningsförfarande och lagring av uppgifter måste ske på ett betryggande sätt.

Inför definition av allriskperspektiv och tydliggör genomförandet av övergripande riskanalyser (3 kap. 1 §)

Förslaget anger i 3 kap. 1 § att ”Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken”.

Förslaget saknar en definition av vad ett allriskperspektiv innebär, vilket medför ett utrymme för osäkerhet och olika tolkningar. I direktivet till utredningen finns en sådan definition som bör föras in i lagtexten.

UPPSALA UNIVERSITET

REMISSVAR

2024-05-28 Dnr UFV 2024/477

Av delbetänkandets beskrivning av riskhanteringsåtgärder framgår att begreppet ”proportionella” innebär att hänsyn ska tas till verksamhetens grad av riskexponering, storlek, sannolikhet för att incidenter inträffar och deras allvarlighetsgrad, inbegripa samhälleliga och ekonomiska konsekvenser.

Det tas, såvitt Uppsala universitet kan bedöma, ingen hänsyn till organisationens komplexitet, eller att olika delar av en stor organisation - som till exempel ett forskningstungt universitet - innehåller vitt skilda områden med olika förutsättningar och risker, olika grad av riskexponering och varierande konsekvenser.

En övergripande riskanalys med ett allriskperspektiv över ett stort antal nätverks- och informationssystem riskerar att bli mycket omfattande och svårgenomtränglig, alternativt på en så övergripande nivå att risker, som är vitala för en del av verksamheten men inte påverkar andra delar eller samhället i stort, inte kommer att kunna tillvaratas eller lyftas fram.

Det är utifrån förslaget mycket svårt bedöma hur omfattande den övergripande riskanalysen ska vara och vilken nivå som är rimlig för ett allriskperspektiv. Breda lärosäten behöver mera vägledning och mera stöd i tolkningen av dessa aspekter.

En omfattande riskanalys kommer sannolikt att innehålla stora mängder känslig sekretessbelagd information av en hög detaljeringsgrad om den ska inkludera de största riskerna och åtgärderna för samtliga system, inklusive system som används av enstaka forskare, system som tillverkas av studenter för laborativa ändamål i studier, system för utbildning, administrativa system, stora forskningsinfrastrukturer, system som delas mellan olika lärosäten, molntjänster och andra tjänster hos olika leverantörer, med mera.

Åtgärderna kommer medföra kraftigt ökande kostnader och ökande administration om alla säkerhets-/riskhanteringsåtgärder ska införas inom all verksamhet, eftersom åtgärderna inte kommer att skydda tillräckligt där det behövs genomgående höga skyddsnivåer, samtidigt som det blir orimligt höga krav på åtgärder inom delar som inte har behov av skydd.

Uppsala universitets arbete med riskanalyser för system, görs i nuläget på informationssystemförvaltningsnivå för administrativa och utbildningssystem, vilka kan aggregeras till en övergripande nivå, samt på systemnivå för de system i kärnverksamheten som inte används som laborativa eller i studiesyfte. Det innebär att riskerna fortfarande ägs och hanteras ute i verksamheten bland systemförvaltarna, vilket är arbetssätt som underlättar för planering, revidering och uppföljning.

Uppsala universitet föreslår att föreskrifterna tydliggör att den övergripande riskanalysen kan vara aggregerad från olika delar av verksamheten, för både ett övergripande perspektiv och effektiv hantering

UPPSALA UNIVERSITET

REMISSVAR

2024-05-28 Dnr UFV 2024/477

med åtgärder som införs utgående från risknivåerna i respektive del av verksamheten.

Förtydliga regelbundenheten av obligatoriska och frivilliga utbildningar (3 kap. 3 §)

Förslaget anger i 3 kap 3 § ”Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.”

Av förslaget framgår att ledning ska genomgå utbildning, medarbetare erbjudas utbildning, och att tillsynsmyndighet får meddela föreskrifter om utbildning.

Eftersom detaljer om regelbundenhet och innehåll saknas, är vår bedömning att kommande föreskrifterna behöver konkretiseras, både med avseende på vilken regelbundenhet utbildning ska ske, samt detaljeringsnivå på utbildningen, eftersom cybersäkerhetslagens angivna riskhanteringsåtgärder var för sig är omfattande och kräver vissa förkunskaper om informationssäkerhetsarbete.

Inom det systematiska arbetsmiljöarbetet finns krav på att organisationer med regelbundenhet ska erbjuda samtliga anställda utbildning, inom bland annat brandskydd. Uppsala universitet ser gärna liknande krav vad gäller informations- och cybersäkerhet.

Uppsala universitet anser att utbildning inom informationssäkerhetsarbete i allmänhet och riskhanteringsåtgärder i synnerhet, lämpligen sker inom respektive myndighet, utifrån den faktiska situation och de faktiska risker som finns där, med stöd och vägledning från tillsynsmyndighet(-er).

I dagsläget utbildar och informerar Uppsala universitet konsistoriet (styrelsen) och universitetsledningen gällande myndighetens säkerhetsarbete, inklusive informationssäkerhet. Universitetet utbildar även medarbetarna, bland annat i grundläggande informationssäkerhet. Ansvaret för den tänkta framtida utbildningen i riskhanteringsåtgärder bör hanteras på likartat sätt.

Uppsala universitet föreslår att det förtydligas i förordning eller föreskrift med vilken regelbundenhet obligatoriska och frivilliga utbildningar ska ske. Det bör utfärdas rekommendation att utbildningar ska genomföras inom respektive verksamhetsutövare, med stöd och vägledning från relevant tillsynsmyndighet .