Svar via e-post:
fi.remissvar@regeringskansliet.se
fi.ofa.dis.remisser@regeringskansliet.se

Remissvar rörande betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

Linköpings universitet (LiU) har beretts tillfälle att yttra sig över *betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)*.

Spridning av information om sårbarheter och incidenter är en av de viktigaste aspekterna av att förebygga framtida incidenter. Informationen är inte viktig enbart för de direkt berörda, utan för alla samhällsaktörer så att de kan lära sig och förbättra sin cybersäkerhet.

Betänkandet föreslår förändringar i offentlighets- och sekretesslagen som innebär att uppgifter i sårbarhets- och incidentrapporter ska omfattas av sekretess med omvänt skaderekvisit (stark sekretess) i 40 år samt att strikt tystnadsplikt gäller för dessa uppgifter.

Linköpings universitet anser förslaget är för långtgående, riskerar leda till försämrad cyberresiliens, att en 40-årig sekretess är för lång, och att de bestämmelser om konfidentialitet som finns i cyberresiliensförordningen är tillräckliga.

De föreslagna bestämmelserna om sekretess och tystnadsplikt riskerar leda till *försämrad* cyberresiliens.

Linköpings universitet ser en påtaglig risk att bestämmelserna om sekretess och tystnadsplikt som föreslås skull hämma samverkan och informationsspridning inom cybersäkerhetsområdet och därmed leda till *försämrad* cyberresiliens, i strid med cyberresiliensförordningens mål.

Trots att förslaget medger vissa möjligheter för CSIRT-enheten att meddela allmänheten eller användare av de berörda produkterna, ger det upphov till såväl direkta rättsliga hinder som osäkerhet kring vilken information som får spridas, och därmed för det informationsflöde som krävs för en bibehållen cyberresiliens.

Sekretessen enligt föreslagna 18 kap. 8 d § OSL gäller hos varje myndighet som förfogar över uppgifter ur sårbarhets- eller incidentrapporter, inte enbart hos CSIRT-enheten. Eftersom sekretessen är knuten enbart till uppgiftens förekomst i en rapport träffar tystnadsplikten alla offentliganställda, även om de fått tillgång till uppgiften från helt andra källor. Den föreslagna ändringen av 18 kap. 19 § OSL undantar dessutom tystnadsplikten från meddelarfriheten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen, en av de starkaste möjliga inskränkningarna.

Något utrymme för det viktiga informella informationsutbyte som bär upp cybersäkerhetssamverkan finns inte: generalklausulen i 10 kap. 27 § OSL är enligt förarbetena avsedd att tillämpas restriktivt och bär inte rutinmässig samverkan, och 10 kap. 28 § OSL kräver en lagstadgad uppgiftsskyldighet som saknas i dessa sammanhang.

De föreslagna bestämmelserna skulle därför skapa osäkerhet hos offentliganställda, troligen även hos CSIRT-enheten, kring vilken information man får förmedla, och eftersom den föreslagna tystnadsplikten är så strikt att den inskränker meddelarfriheten så kommer många att välja den säkra vägen: att inte dela information i många av de sammanhang som i dag ligger till grund för samhällets cyberresiliens.

Den föreslagna sekretessen gäller under för lång tid.

Förslaget till bestämmelser anger att sekretessen ska gälla i 40 år, närmast en evighet på internet och i cybersäkerhetsområdet. För att sätta det i perspektiv, låt oss blicka tillbaka på internet 1986.

- Apple hade lanserat den första Mac:en bara två år tidigare, och Microsoft hade lanserat Windows 1.0 ett år tidigare. Windows 3.1, den första version med riktig spridning, skulle inte se dagens ljus på över fem år.
- Sverige var inte anslutet till Internet, utan det var först två år senare som Sverige genom Sunet och Nordunet anslöts till USA. Tidigare hade endast någon enstaka forskare varit ansluten.
- Det var också två år senare som den första stora cybersäkerhetsincidenten inträffade – den beryktade internetmasken – som påverkade stora delar av internet och var upphovet till den samverkan inom CSIRT-området som är så viktig i dag.
- Webben skulle inte nå utanför CERN förrän sju år senare, 1993, då även Sveriges första webbplats skapades. Microsoft skulle inte släppa sin första webbläsare förrän nio år senare.
- Det var tio år innan Ines Uusmann lär ha yttrat att ”internet är en fluga som kanske blåser förbi” och tio år innan modemet och internetabonnemanget blev årets julklapp.

Med 40 års sekretess hade vi än i dag inte fritt kunnat diskutera sårbarheter i tidiga

versioner av Windows, de första webbservrarna eller webbläsarna, den första versionen av Internet Explorer eller diskutera detaljer kring det första storskaliga cyberangreppet.

Det är värt att notera att det inte gör någon skillnad om sekretessen är med rakt eller omvänt skaderekvisit eftersom det inte råder några tvivel om att den som använder en sårbar programvara, även om den är närmare 40 år gammal, kan lida skada om information om sårbarheterna sprids.

Förordningens möjligheter till konfidentialitet är tillräckliga.

Linköpings universitet håller med om att det behöver finnas möjligheter i regleringen att hålla viss information konfidentiell under en tid, men att en nationell pålaga med omvänt skaderekvisit och strikt tystnadsplikt med en 40-årsgräns är för långtgående och inte i linje med de tydligt riskbaserade principerna som underbygger den svenska cybersäkerhetslagen och all EU-reglering inom cybersäkerhetsområdet.

Cyberresiliensförordningen innehåller redan ett riskbaserat system för konfidentialitet: artikel 14.4 b låter tillverkaren ange hur känslig den anmälda informationen är, artikel 15.5 ålägger CSIRT-enheten att säkerställa konfidentialitet för frivilligt rapporterad information, och artikel 63 skyddar företagshemligheter, nationell säkerhet och integriteten i rättsliga förfaranden. Artikel 16.2 ger möjlighet att skjuta upp spridning av anmälningar på motiverade cybersäkerhetsskäl under den tid som är absolut nödvändig, och artikel 17.5 säkerställer att sårbarheter förs in i den europeiska sårbarhetsdatabasen så snart en säkerhetsuppdatering finns. Detta är ett proportionellt system som väger skyddsbehov mot informationsflöde.

Handläggningen av beslutet

Beslut i detta ärende har fattats av Digitaliseringsdirektör Joakim Nejdeby, efter föredragning av enhetschefen David Byers.

Joakim Nejdeby

David Byers

Sändlista:

Mottagare av remissvaret enligt ovan
Internrevisionen
Dokument- och arkivenheten (original)