MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Yttrande

Diarienummer: 2024–1610

Klassificerings-ID: 3.5.2

Datum: 2024-05-21

Finansdepartementet

fo.remissvar@regeringskansliet.se

Nya regler om cybersäkerhet (SOU 2024:18)

dnr Fö2024/00496

Myndigheten för digital förvaltning (Digg), som har i uppdrag att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig, lämnar följande synpunkter.

Sammanfattning

Digg tillstyrker delbetänkandet samt bedömningar och förslag som utredningen presenterar om genomförande av NIS2-direktivet och

- välkomnar förslaget om hur Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) ska implementeras i Sverige,
- anser också att de olika förslag som Myndigheten för samhällsskydd och beredskap (MSB) lämnat i sitt remissvar (MSB 2024-03843-4, den 10 april 2024), i de delar som inte specifikt avser MSB:s egen verksamhet, noggrant behöver beaktas i det fortsatta lagstiftningsarbetet,
- anser att vissa delar av förslaget behöver analyseras djupare och övervägas ytterligare i det fortsatta lagstiftningsarbetet,
- lämnar ett antal generella synpunkter på bedömningar och förslag i delbetänkandet som Digg anser behöver analyseras vidare i fortsatt arbete.

Generella synpunkter

Digg anser att följande avsnitt i delbetänkandet behöver ses över i fortsatt arbete

7.1.2 Riskhanteringsåtgärder – Del 1

I avsnittet samt i förslaget till cybersäkerhetslag (3 kap. 1 § i förslaget) föreslås att de riskhanteringsåtgärder som ska vidtas ”ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken”.

Sammantaget menar utredningen att åtgärderna ska vara proportionella i förhållande till risken och att det bör följa av lagtexten. Att åtgärderna även ska vara lämpliga i förhållande till risken blir då enligt utredningens mening överflödigt, eftersom det inte tillför något.

- Digg har synpunkter på förslagets utformning samt bedömningen att det är överflödigt att ange att åtgärderna ska vara lämpliga, bör framgå av lagtexten.

Lämpligheten handlar enligt Diggs uppfattning om att vidta rätt åtgärd för en viss specifik risk, medan proportionaliteten handlar om hur omfattande åtgärden måste vara för att motverka eller eliminera risken. Även om båda begreppet i någon mening handlar om lämplighet så finns här en skillnad som Digg tror kan vara viktig att framhäva i lagtexten. Om det inte anses att både lämplig och proportionerlig ska framgå av lagtexten, så förordar Digg att nyansskillnaden mellan begreppen behöver tydliggöras och förklaras i det kommande vägledande arbetet.

7.1.2 Riskhanteringsåtgärder – Del 2

Vidare anger utredningen (på sid. 194) att åtgärder enligt artikel 21.2 i NIS2-direktivet minst ska omfatta strategier för riskanalys och informationssystemens säkerhet.

- Digg har synpunkter på denna bedömning och föreslår att strategier för riskanalys och informationssystemens säkerhet samt strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet uttryckligen ska framgå i förslaget till cybersäkerhetslag, i dess 3 kap. 1 §.

Strategier innefattar långsiktig planering. Och även om sådan långsiktighet ingår i det systematiska informationssäkerhetsarbetet som kommer bedrivas hos verksamhetsutövarna, så förordar Digg att det strategiska, långsiktiga, arbetet rörande riskanalys framgår uttryckligen i den föreslagna cybersäkerhetslagen. Skälet är att långsiktigheten i det strategiska arbetet är en viktig del i att kunna upprätthålla det systematiska arbetssättet över tid. Det blir också enligt Diggs mening inkonsekvent att utesluta strategier i denna del, när dessa framgår i andra delar av bestämmelsen.

7.1.2 Riskhanteringsåtgärder – Del 3

I artikel 21.2 b i NIS2-direktivet anges incidenthantering och driftskontinuitet i punkten c i samma bestämmelse.

- Digg anser i likhet med MSB att det direkt ur lagtexten bör framgå att säkerhetskopiering och krishantering är sådana riskhanteringsåtgärder som ska vidtas.

7.1.2 Riskhanteringsåtgärder – Del 4

Vidare framgår på utredningens sidor 194 - 195 att det av artikeln 21.2 d i NIS2-direktivet följer att säkerhet i leveranskedjan är ett minimikrav. En särskild fråga är då enligt utredningen vad som avses med säkerhet i leveranskedjan, hur många led i kedjan som verksamhetsutövaren ansvarar för.

- Digg vill lyfta fram att det i det praktiska arbetet med riskhantering och systematiskt informationssäkerhetsarbete relativt ofta är nödvändigt att utreda och bedöma flera led bortom det första ledet.

Om inte annat för att avtalsvis, gentemot leverantören i första ledet, kunna reglera vilka riskhanteringsåtgärder samt informations- och it-säkerhetsåtgärder som förstaledsleverantörerna behöver vidta och svara för rörande de följande leverantörsleden. Digg förordar därför att detta återspeglas i det fortsatta författnings- eller vägledningsarbetet.

7.3 Incidentrapportering

Utredningen föreslår att verksamhetsutövaren ska informera kunder som kan antas påverkas av en betydande incident. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot (3 kap. 6 §, sista stycket i förslaget till cybersäkerhetslag).

- Digg föreslår att begreppet ”mottagare” används istället för, alternativt kompletterar, begreppet kunder.

Exempelvis skulle formuleringen ”Kunder och andra mottagare av verksamhetsutövarens tjänster” kunna användas i den aktuella bestämmelsen. Begreppet kunder kan leda tanken till att det måste föreligga någon form av ekonomiskt förhållande eller finnas någon ekonomisk prestation för att få del av en verksamhetsutövares tjänst. Så är inte alltid fallet med tjänster som tillhandahålls av offentliga aktörer. Begreppet mottagare omfattar enligt Diggs mening såväl fysiska som juridiska personer som står i förbindelse med verksamhetsutövaren i egenskap av nyttjare av dess tjänst. Detta rimmar därför bättre med vad NIS2-direktivet anger i artiklarna 32.4 e och 33.4 e. Möjligen kan, istället för begreppet mottagare, begreppet ”fysiska och juridiska personer” användas så att ett tillägg görs i den aktuella bestämmelsen lydande ”fysiska och juridiska personer som mottar verksamhetsutövarens tjänster” alternativt ”… som använder verksamhetsutövarens tjänster.”. Ett sådant uttryckssätt skulle då ligga i linje med 5 kap. 7 § andra stycket i förslaget till cybersäkerhetslag.

8.4.5 Föreskrifter

I avsnittet 8.4.5 för utredningen resonemang om för- respektive nackdelar med föreskriftsrätt hos antingen MSB eller de respektive tillsynsmyndigheterna.

- Även om Digg i stort håller med om de bedömningar som utredningen gör i avsnitt 8.4.5 så vill Digg framföra att myndigheten inte är övertygad om att det som utredningen anger om att behovet av en central myndighetsföreskrift inte är lika stort avseende NIS2-direktivet är riktigt.

Tvärtom tror Digg, i likhet med vad utredningen på sidan 228 redogör för att MSB, Säkerhetspolisen, Transportstyrelsen samt Integritetsskyddsmyndigheten framfört till utredningen, att en central myndighetsföreskrift tillsammans med kompletterande ”sektorföreskrifter” kommer ge bättre möjligheter att göra heltäckande åtgärder som behöver vidtas för att efterleva förskrifterna.

- Digg anser därför att en gemensam föreskrift med grundkrav som gäller för samtliga sektorer i syfte att konkretisera de riskhanteringsåtgärder som anges i cybersäkerhetslagen, fortsatt bör övervägas i det arbetet med implementeringen av direktivet.

Under alla omständigheter bedömer Digg att det samarbetsforum som MSB föreslås leda (37 § i förslaget till cybersäkerhetsförordning samt avsnitt 8.4.7 i utredningen) kommer att vara viktigt.

Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. Digg tror att skillnader och likheter mellan den gemensamma föreskriften och de sektorsspecifika föreskrifterna, samt tolkning och tillämpning av de genomförandebeslut som EU-kommissionen förväntas meddela, kommer finna ett naturligt diskussionsforum där. Givet det antal tillsynsmyndigheter – liksom det som utredningen uttrycker på sidan 242 om verksamhetsutövare som kommer stå under tillsyn av flera tillsynsmyndigheter - som kommer att komma till stånd så tror Digg att samarbetsforumets betydelse kommer att öka. Digg stärks än mer i den uppfattningen när utredningen beskriver effekterna av det nu redan existerande forumet (avsnitt 8.3.2 och 8.4.7) där också utredningen själv uttrycker en tro om ett ökat behov.

8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

Utredningen föreslår bland annat att den som står under tillsyn på begäran ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen och att tillsynsmyndigheten i den omfattning det behövs för tillsynen ska ha rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten (4 kap. 4-5 §§ i förslaget till cybersäkerhetslag).

- Digg föreslår att det i det fortsatta arbetet med implementeringen övervägs om dessa befogenheter också ska innefatta åtkomst till it-system och att detta ska framgå direkt av lagtexten.

Det förefaller enligt Diggs mening rimligt, med tanke på vad som ska granskas vid tillsyn, att kunna granska hur riskhanteringsåtgärder fått genomslag i praktiken, till exempel i en verksamhetsutövares it-infrastruktur. Det förefaller också ligga i linje med vad utredningen anför på

sid. 239 och vad som framgår i 4 kap. 9 § i förslaget till cybersäkerhetslag, nämligen att tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av lagen, samt att sådana säkerhetsskanningar är en typ av sårbarhetsskanning som kan göras på verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter eller osäkert konfigurerade delar av systemet. Vidare skriver utredningen där att sårbarhetsskanningar normalt sker med automatiserade verktyg som identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer genom att matcha dem mot redan kända systembrister och att detta antingen kan göras på allmänt tillgängliga nätverks- och informationssystem eller med olika nivåer av åtkomst till systemen.

9.4.2 Vad ska beaktas särskilt vid val av sanktion och utformningen av dem?

Uppkommen (risk för) skada på sidan 258

Utredningen anger att omfattningen av den skada, eller risk för skada, som har uppstått till följd av överträdelsen är en faktor som ska beaktas särskilt.

- Digg delar i huvudsak utredningens bedömningar och att ett brett perspektiv bör anläggas, men vill lyfta fram att ”risk för skada” inte är en faktisk skada, bara en sannolikhet för att en skada – som kanske inte inträffar – kan komma att inträffa.

Digg befarar att ”risk för skada” kan bli svårt att ha som bedömningsgrund vid val av ingripande från tillsynsmyndighetens sida. Hur pass allvarlig ska en risk behöva vara, för att utgöra en överträdelse, om inget rent faktiskt har hänt till följd av risken? Detta hänger, precis som utredningen anför på samma sida 258, tätt samman med ”*Vidtagna åtgärder för att minimera skadan*”. Digg anser, liksom Digg tolkar det som att utredningen också gör under rubriken ”*Vidtagna åtgärder för att minimera skadan*” på sidorna 258 och 381, att överträdelsen av reglerna bör vara att en verksamhetsutövare, vid en uppkommen risk, inte vidtagit skyndsamma och verkningsfulla åtgärder för att förhindra realiserandet av risken. Digg rekommenderar att detta förtydligas i det fortsatta implementerings- och vägledningsarbetet.

Detta yttrande har beslutats av generaldirektör Anna Eriksson. I den slutliga handläggningen har jurist Lars Söderberg, säkerhetschef/säkerhetsskyddschef Johan Gellerstedt, rättschef Linn Kempe och avdelningschef tillika ställföreträdande generaldirektör Chanett Edlund deltagit.

Föredragande har varit informationssäkerhetsspecialist Anders Nordlander.

Anna Eriksson