scrive.

Regeringskansliet
Försvarsdepartementet
111 52 Stockholm

Diarienummer Fö2024/00496

Remissvar till delbetänkande En säker och tillgänglig statlig e-legitimation (SOU 2024:18)

Scrive grundades 2010 och idag använder fler än 10 000 organisationer Scrive för att automatisera sina dokument- och avtalsprocesser med lösningar för elektroniska underskrifter och identifiering. Våra kunder innefattar några av Sveriges största industribolag, banker och telekomoperatörer. Scrive tillhandahåller tjänster som föreslås omfattas av den nya cybersäkerhetslagen och tillhandahåller även tjänster till kunder som kommer utgöra verksamhetsutövare.

Vi har tagit del av delbetänkandet från Utredningen om genomförande av NIS2-direktivet och ställer oss överlag positiva till utredningens förslag.

Scrive AB
Grev Turegatan 11A
114 46 Stockholm

Datum
2024-05-28

Ärende
Fö2024/00496

Scrive ser dock behov av:

- en begränsning av vilka nätverks- och informationssystem som ska omfattas av regleringen,
- att det i lagen förtydligas hur verksamhetsutövare som både klassificeras som viktiga och väsentliga ska behandlas,
- att en verksamhetsutövare som tillhandahåller både molntjänster och betrodda tjänster endast ska klassificeras som tillhandahållare av betrodda tjänster,
- att det införs bestämmelser om sammanhållen incidentrapportering för tillhandahållare av betrodda tjänster under NIS2-direktivet och den reviderade eIDAS-förordningen, samt
- att tillsynen över icke-kvalificerade tillhandahållare av betrodda tjänster under cybersäkerhetslagen anpassas till eIDAS-förordningen.

Nedan följer ett antal synpunkter och förslag på ytterligare förbättringar av utredningens förslag:

5.2.2 Verksamhetsutövare

Utredningen föreslår att hela verksamhetsutövarens verksamhet ska omfattas av den föreslagna lagens krav, utan en avgränsning till de nätverks- och informationssystem som används för att tillhandahålla den reglerade tjänsten. Att inte införa en sådan avgränsning kommer att innebära omfattande krav också på de delar av verksamheten som inte är av sådan betydelse för samhället eller ekonomin att de ska regleras. Vi tror därför att kraven kommer att få en betydande negativ inverkan på svensk konkurrensförmåga och ekonomisk effektivitet. Om två bolag som konkurrerar med närmast identiska tjänster omfattas av olika cybersäkerhetskrav – till följd av att ett bolag även tillhandahåller andra tjänster – kommer det nämligen att resultera i olika prissättningar.

Det kommer även att innebära att verksamhetsutövare behöver avdela resurser för att bland annat göra riskanalyser av och vidta riskhanterings-åtgärder för system som helt saknar koppling till och betydelse för den reglerade tjänsten. Scrive använder exempelvis en molntjänst för internutbildning av personal. Skulle den tjänsten upphöra att fungera skulle det inte påverka Scrives förmåga att tillhandahålla betrodda tjänster. Utbildningsplattformen har inte heller några tekniska kopplingar till de system som används för att tillhandahålla våra betrodda tjänster.

Scrive är inte heller av uppfattningen att det i direktivet inte finns utrymme för att låta endast en del av en entitets verksamhet omfattas. Utifrån Scrives tolkning medger NIS2-direktivet istället precis samma möjlighet som NIS1-direktivet gör. Nämligen att låta kraven på riskhanteringsåtgärder omfatta endast den typ av verksamhet som uttryckligen utpekas. I artikel 21 i NIS2-direktivet anges att entiteter ska vidta "lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster". Scrive menar att termen verksamhet här syftar på de i bilagorna utpekade verksamheterna. Om avsikten med NIS2-direktivet istället hade varit att verksamhetsutövarens samtliga nätverks- och informationssystem skulle omfattas av kraven i artikel 21 så hade artikeln inte innehållit den tydliga avgränsningen: ″som de använder för sin verksamhet eller för att tillhandahålla sina tjänster″. Scrive menar alltså, i motsats till utredningen, att direktivet avser att endast vissa nätverks- och informationssystem ska omfattas av kraven på riskhanteringsåtgärder.

Scrive anser därför att det i cybersäkerhetslagen måste införas en begränsning av vad som kommer att omfattas av lagens krav, liknande formuleringen "[...] som de använder för att tillhandahålla samhällsviktiga tjänster" som idag finns i NIS-lagens 13 §.

5.2.12 Enskilda verksamhetsutövare

Utredningen föreslår inga ytterligare förtydliganden kring de sektorsavgränsningar som finns i NIS2-direktivets bilagor. Scrive anser att det i vart fall finns ett behov av att förtydliga hur vissa typer av entiteter förhåller sig till varandra när det gäller klassificering. Så gäller till exempel förhållandet mellan de olika typerna av entiteter: leverantörer av molntjänster respektive tillhandahållare av betrodda tjänster. Scrive tillhandahåller en lösning för elektroniska underskrifter och vi bedömer preliminärt att hela eller delar av vår lösning utgör en molntjänst. Det är dock oklart om en sådan tjänst ska bedömas som:

- en molntjänst,
- en en betrodd tjänst, eller
- som både en molntjänst och en betrodd tjänst.

En betrodd tjänst är en mer specifik tjänstetyp än en generell molntjänst, vilket framgår redan av att de regleras särskilt. Scrive anser därför att den betrodda tjänsten här bör konsumera molntjänsten. En molntjänst för framställande av elektroniska underskrifter bör följaktligen endast betraktas som en betrodd tjänst, vilket behöver förtydligas.

6.1 Väsentlig eller viktig

Enligt direktivet och utredningens förslag ska kvalificerade leverantörer av betrodda tjänster klassificeras som väsentliga verksamhetsutövare. Samtidigt är det tänkbart att sådana leverantörer tillhandahåller även andra tjänster som täcks av bilaga 1 eller 2. Tillhandahåller verksamhetsutövaren till exempel även molntjänster och dessutom klassificeras som ett medelstort företag kommer verksamhetsutövaren att klassificeras som både väsentlig och viktig. Utredningens förslag innehåller inga närmare regler för hur en sådan konflikt ska hanteras.

Post- och telestyrelsen (PTS) föreslås bli tillsynsmyndighet över både tillhandahållare av betrodda tjänster och leverantörer av molntjänster. Det kan inte uteslutas att PTS vid en planerad tillsyn av den betrodda tjänsten erhåller information om molntjänsten. Myndigheten har då inhämtat information om molntjänsten genom planerad tillsyn, samtidigt som viktiga verksamhetsutövare endast omfattas av händelsestyrd tillsyn.

Konflikter kan även uppstå i frågor om vilka sanktionsåtgärder och sanktionsbelopp som kan tillämpas på verksamhetsutövaren.

Mot den bakgrunden anser Scrive att det i lagen bör införas bestämmelser om hur sådana konflikter ska behandlas.

7.3 Incidentrapportering

Genom NIS2 och eIDAS2 delas incidentrapporteringskraven för tillhandahållare av betrodda tjänster upp mellan två regleringar. NIS2 innehåller krav på rapportering av betydande incidenter som drabbar nätverks- och informationssystem. Vidare ställer eIDAS2 krav på rapportering av incidenter för att “hantera rättsliga, affärsmässiga, operativa och andra direkta eller indirekta risker”. I skäl 50 i eIDAS2 anges att: “[k]raven och rapporteringsskyldigheterna för hanteringen av riskerna för cybersäkerheten enligt [NIS2] bör ses som komplement till de krav som införs för tillhandahållare av betrodda tjänster enligt denna förordning”.

Förutsatt att inga ändringar sker vad gäller ansvar hos myndigheter avseende incidentrapportering kommer Scrive alltså att vara skyldigt att

rapportera incidenter för en tjänst i två olika incidentrapporteringssystem, med två olika rapporteringsvägar, till två olika myndigheter och sannolikt med två olika rapporteringsformulär. Detta trots att det är en och samma myndighet som är slutlig mottagare och som kommer att ha tillsynsansvar över båda incidentrapporterna. Som tillhandahållare av betrodda tjänster kommer vi dessutom att behöva rapportera inom 24 timmar, istället för inom 72 timmar, vilket skapar ytterligare osäkerhet.

Ett sådant system skapar en onödig komplexitet och leder till en uppenbar risk för fördröjning av incidentrapporteringen. Tillhandahållare av betrodda tjänster kommer behöva avsätta resurser för att fastställa var incidenten ska rapporteras och vilken information som ska ta vilken rapporteringsväg, istället för att använda resurserna för att hantera incidenten.

Scrive anser därför att incidentrapportering enligt NIS2 och eIDAS bör ske på ett sammanhållet sätt. Oaktat om rapporteringen sker direkt till PTS, eller om de rapporteras via MSB, bör rapportering för båda regelverken ske till samma myndighet och med samma metoder och samma innehåll.

8 Tillsyn

Avgörande för när tillsyn kan göras av en verksamhetsutövare beror på om det är fråga om en viktig eller väsentlig verksamhetsutövare. En kvalificerad tillhandahållare av betrodda tjänster kommer alltid att utgöra en väsentlig verksamhetsutövare, medan storleken på verksamhets-utövaren blir avgörande för en icke-kvalificerad tillhandahållare.

Avgörande för om en tillhandahållare av betrodda tjänster kan bli föremål för tillsyn på förhand eller i efterhand enligt eIDAS är om den har status som kvalificerad.

En icke-kvalificerade tillhandahållare av betrodda tjänster kommer alltså enligt cybersäkerhetslagen att kunna vara föremål för tillsyn antingen i förhand eller i efterhand (beroende på dess storlek), samtidigt som den endast kan vara föremål för tillsyn i efterhand enligt eIDAS.

Med det allriskperspektiv som cybersäkerhetslagen föreslås ha avseende riskhantering bedömer Scrive att det kommer att kunna uppstå stora utmaningar i att avgöra exakt vilket tillsynsmandat PTS kommer att ha över icke-kvalificerade tillhandahållare. I och med att eIDAS är en förordning och NIS2 är ett direktiv är vår uppfattning att NIS2 aldrig kan utöka tillsynen över det som eIDAS reglerar.

Beslut om detta remissvar har fattats av chefsjurist Peter Carlstedt efter föredragning av bolagsjuristerna Linus Kilander Xu och Mathias A. Bjerkhaug. I arbetet med remissvaret har även den seniora informationssäkerhetsexperten Björn Hesthamar deltagit.



Peter Carlstedt	Linus Kilander Xu	Mathias A. Bjerkhaug
Chefsjurist	Bolagsjurist	Bolagsjurist

Scrive AB
Grev Turegatan 11A
114 46 Stockholm

Datum
2024-05-28

Ärende
Fö2024/00496

Verification

Transaction 09222115557518551191

Document

Scrive AB - Remissvar SOU 2024_18 - Google Docs
Main document
6 pages
Initiated on 2024-05-28 16:16:31 CEST (+0200) by Linus Kilander Xu (LKX)
Finalised on 2024-05-28 16:43:24 CEST (+0200)

Signatories

Linus Kilander Xu (LKX)
Scrive AB
Company reg. no. 556816-6804
linus.kilanderxu@scrive.com

Signed 2024-05-28 16:19:00 CEST (+0200)

PC (P)
Scrive
peter@scrive.com

Signed 2024-05-28 16:43:24 CEST (+0200)

MB (M)
Scrive
mathias.bjerkhaug@scrive.com

Signed 2024-05-28 16:26:29 CEST (+0200)