CERTEZZA

Försvarsdepartementet
103 33 STOCKHOLM

Ert diarienummer: Fö2024/00496

2024-05-27

Nya regler om cybersäkerhet, SOU 2024:18

Om Certezza

Certezza är ett oberoende informations- och cybersäkerhetsföretag som erbjuder spetskompetens till näringsliv och offentlig sektor. Vår vision är att Certezza bidrar till att bygga ett säkert och robust samhälle genom att vara marknadens främsta informations- och cybersäkerhetspartner.

Certezza är flitigt engagerad som kvalificerad strategisk rådgivare inom säkerhetsskydd, juridik, dataskydd, cybersäkerhet, informationssäkerhet, it-säkerhet, Identitets- och åtkomsthantering (IAM), kryptering och infrastruktur för kryptering (PKI), säkerhetsgranskningar, säkerhetsrevisioner och penetrationstestning samt support och säkerhetsövervakning (säkerhetscenter).

Certezzas sammanfattande synpunkter

- Lagstiftningen bör endast omfatta den del av verksamheterna som tillhandahåller direktivsrelevanta tjänster. Däremot bör självklart ledningens ansvar att gälla fullt ut oavsett om verksamheten endast till viss del hör till en sektor som omfattas av direktivet.
- Sektorn offentlig förvaltning behöver förtydligas. Kommunala och regionala myndigheter bör omfattas av lagstiftningen, men det kan ifrågasättas om det finns tillräckligt beredningsunderlag för att genomföra detta nu.
- Fler statliga myndigheter borde omfattas av regelverket. Endast säkerhetskänslig verksamhet såsom den definierats i verksamhetsutövarens säkerhetskyddsanalys borde undantas.
- Antalet tillsynsmyndigheter borde vara mycket färre och föreskrifter borde tas fram av betydligt färre myndigheter. Sverige riskerar att översvämmas av överlappande föreskrifter och myndighetsutövning utan samordning och spretig praxis. Det blir onödigt komplicerat för ett område som har behov av högre grad av enkelhet. Det kan också innebära större kostnader för verksamhetsutövares utan att cybersäkerhetsnivån höjs.
- Byt ordet riskhanteringsåtgärder mot säkerhetsåtgärder.
- Flera säkerhetsåtgärder enligt direktivet har inte införts i förslaget, men de bör ingå i lagstiftningen.

Certezza föreslår att regeringen omgående tillsätter en utredning med uppdrag att lämna förslag på hur och i vilken omfattning kommuner och regioner kan omfattas av cybersäkerhetslagen och hur tillsynen kan bedrivas av en eller några få myndigheter.

Detta remissvar har beslutats av Certezzas ledningsgrupp efter föredragning av chefsjurist Andreas Dahlqvist.

Kornhamnstorg 61
SE-111 27 Stockholm
Sweden

Telefon +46 (0)8 791 92 00
www.certezza.net

Inledning

NIS-direktivet och NIS2-direktivet har varit, och är mycket viktiga för att åstadkomma en höjning av cybersäkerhetsnivån i samhället. Därför är det också mycket viktigt att implementeringen av NIS2-direktivet genomförs på ett effektivt och lämpligt sätt som leder till de önskade resultaten. En stor utmaning med regelverket är att det hämtar sitt innehåll från många olika EU-rättsakter och det underlättar tyvärr inte för de som ska arbeta med regelverket. Certezza vill gärna hjälpa till så att de nya reglerna om cybersäkerhet blir så bra som möjligt.

Allmänna synpunkter

Certezza ställer sig mycket positiv till det nya regelverket som är mycket viktigt för att höja cybersäkerhetsnivån i Sverige. Samtidigt är det viktig att ta detta tillfälle i akt att säkerställa ett heltäckande och enkelt regelverk som är lätt att tillämpa. Cybersäkerhet uppfattas komplicerat för dem som inte arbetar med det på daglig basis. Eftersom regelverket ska tillämpas av många verksamhetsutövare som inte har cybersäkerhet eller juridik som sin dagliga sysselsättning är det viktigt att det är lätt att förstå och tillämpa. Det vore bra om lagstiftaren undviker hänvisningar till andra lagar och EU-rättsakter i så stor utsträckning som möjligt eftersom det inte är ovanligt att sådan lagstiftningsteknik gör att verksamhetsutövare missar viktigt innehåll. Det är huvudsakligen jurister som har den metodologiska förmågan att effektivt leta upp olika rättsakter och hämta innehåll från olika rättskällor.

Det vore önskvärt om cybersäkerhetsregleringen utgör en grundläggande basplatta för alla verksamheter i Sverige, från myndigheter till enskilda verksamhetsutövare. Vi behöver höja cybersäkerhetsnivån generellt i samhället och inte bara i vissa sektorer. I vart fall bör alla samhällsviktiga aktörer omfattas. Certezza tror inte på att särskilt peka ut säkerhetskänsliga verksamheter i lagstiftning. Det vore bättre att låta de delar av verksamheten som är säkerhetskänslig, oavsett var den bedrivs – oavsett omfattning – undantas från regelverket, eller i vart fall undantas från viss tillsyn. Ett alternativ skulle vara att säkerställa att den myndighet som har tillsyn över säkerhetsskyddet också har tillsyn över cybersäkerhetslagen, då skulle den myndigheten kunna navigera tillsynen oavsett om det är cybersäkerhetslagen eller säkerhetsskyddslagen som är tillämplig och kan hantera gränsdragningsproblem på ett lämpligare sätt.

Vi behöver bättre regler, inte fler. Certezza ser med oro på förslaget att alla tillsynsmyndigheter ska ta fram sektorsspecifika föreskrifter som ska gälla för en viss verksamhet eller viss sektor. Det riskerar att översvämma Sverige med cybersäkerhetsregelverk av olika kvalité och räckvidd samt till viss del överlappa varandra för verksamhetsutövare som har verksamhet i flera sektorer. Staten har hittills inte visat prov på felfri samordning när det gäller detta.

Inom cybersäkerhet är förtroende och tillit avgörande och vi behöver därför hjälpas åt att skapa ett regelverk som är sammanhållet samt lätt att förstå och tillämpa därför ser Certezza med tillförsikt fram emot det fortsatta lagstiftningsarbetet

Certezzas detaljerade synpunkter per avsnitt i kronologisk ordning

När det gäller de olika avsnitten i betänkandet har Certezza följande synpunkter.

1 Författningsförslag

1.1 Förslag till lag om cybersäkerhet

1 kap Inledande bestämmelser

Utredningens förslag	*Certezzas förslag*
Lagens syfte **1 §** Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.	**Lagens syfte** **1 §** Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå *i samhället*.

Skälen till Certezzas förslag:
NIS2-direktivets artikel 1.1 anger att direktivet fastställer åtgärder för att säkerställa en hög gemensam cybersäkerhetsnivå i unionen. Utredningen har ambitionen att syftet ska följa direktivet semantiskt. Certezza delar den ståndpunkten, men såsom utredningen har formulerat det blir meningen ofullständig. Certezza föreslår därför att syftet förtydligas något i linje med NIS2-direktivets semantik, i första hand med subjektet ”i samhället” men man kan även tänka sig ”i Sverige” eller liknande för att meningen ska bli fullständig, se avsnitt 5.1.2.

Uttryck i lagen

Utredningens förslag	*Certezzas förslag*
2 § […] *16. Hanterade säkerhetstjänster:* en verksamhet som utför eller tillhandahåller stöd för annan verksamhet gällande hantering av tjänster som hanterar cybersäkerhetsrisker, *17. Hanterade tjänster:* en verksamhet som erbjuder tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans, […]	**2 §** […] *17. Utlokaliserade säkerhetstjänster:* en verksamhet *som tillhandahåller utlokaliserade drifttjänster* som utför eller tillhandahåller stöd för annan verksamhet gällande hantering av tjänster som hanterar cybersäkerhetsrisker, *16. Utlokaliserade driftstjänster:* en verksamhet som erbjuder tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans, […]

Skälen till Certezzas förslag:
I rättelse 2023/90206 till NIS 2-direktivet framgår det att alla förekomster av ”leverantörer av hanterade tjänster” ska ersättas med ”leverantörer av utlokaliserade drifttjäns-

ter", med nödvändiga anpassningar samt att alla förekomster av "leverantör/leverantörer av hanterade säkerhetstjänster" ska ersättas med "leverantör/leverantörer av utlokaliserade säkerhetstjänster", med nödvändiga grammatiska anpassningar. Denna rättelse får inverkan på hur denna sektor omfattas av regelverket och behöver därför genomgående anpassas i det fortsatta lagstiftningsarbetet, se avsnitt 4.6.

Lagens tillämpningsområde

Offentliga verksamhetsutövare

Utredningens förslag	*Certezzas förslag*
3 § Denna lag gäller för 1. statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges *d*omstolar, 2. region*er* i Sverige *med undantag för regionfullmäktige*, och 3. kommun*er* i Sverige *med undantag för kommunfullmäktige*.	**3 §** Denna lag gäller för 1. statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges *D*omstolar, *med undantag för Domstolsverket*, 2. region*ala myndigheter* i Sverige, och 3. kommun*ala myndigheter* i Sverige.

Skälen till Certezzas förslag:
Riksdagen och de beslutande kommunala församlingarna är inga myndigheter, jfr 1 kap 4 § regeringsformen och 2 kap 5 § tryckfrihetsförordningen. Genom att förtydliga att det är myndigheter som omfattas behöver man inte undanta de beslutande församlingarna. I annat fall borde man i punkten 1 ange staten med undantag för riksdagen m.fl. Utredningen skriver att Domstolsverket ska ingå och att myndigheten inte ingår i begreppet Sveriges Domstolar. På Sveriges Domstolars hemsida framgår emellertid att " Domstolsverket är en statlig myndighet inom Sveriges Domstolar […]".[1] Det behöver således förtydligas att Domstolsverket ska omfattas av regelverket.

Enskilda verksamhetsutövare

Utredningens förslag	*Certezzas förslag*
4 § […] Regeringen eller den myndighet regeringen bestämmer får *i föreskrifter* meddela undantag för 3 avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.	**4 §** […] Regeringen eller den myndighet regeringen bestämmer får *besluta om* undantag för 3 avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.

[1] https://www.domstol.se/om-sveriges-domstolar/sa-fungerar-domstolarna/myndigheter-och-namnder/

Skälen till Certezzas förslag:
Certezza ifrågasätter lämpligheten i att meddela enskilda undantag i form av föreskrifter. Föreskrifter bör vara generellt tillämpliga och inte användas vid beslut om enskilda undantag. Jfr 4 § i förslag till förordning om cybersäkerhet, avsnitt 1.4, (s. 56 i betänkandet). I annat fall bör ovan nämnda paragraf i förordningen formuleras såsom att myndigheten i föreskrifter får ange enskilda undantag och då skulle föreskriftsrätten kunna framgå av motsvarigheten till 35 § i förslaget till förordning om cybersäkerhet istället.

Utredningens förslag	*Certezzas förslag*
6 § Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder: […] 7. hanterade tjänster, 8. hanterade säkerhetstjänster, eller […].	**6 §** Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder: […] 7. *utlokaliserade drifts*tjänster, 8. *utlokaliserade* säkerhetstjänster, eller […].

Skälen till Certezzas förslag:
Se kommentar ovan rörande rättelse 2023/90206 till NIS2-direktivet.

Utredningens förslag	*Certezzas förslag*
8 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 omfattas också av lagen om, […] Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter.	**8 §** Verksamhetsutövare som uppfyller kraven i *1 kap* 4 § med undantag för storlekskravet i *1 kap 4 §* 3 omfattas också av lagen om, […] Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter *om vilka verksamheter som enligt 1-3 oavsett storlekskravet ska omfattas av lagen.*

Skälen till Certezzas förslag:
Förtydliga hänvisningen till storlekskravet i 3:e punkten fjärde paragrafen samma kapitel.

Den föreslagna delegationsbestämmelsen är ofullständig och behöver förtydligas. I avsnitt 5.2.13 saknas vidare resonemang kring delegationsbestämmelsen i denna paragraf. Det är därför något otydligt vad som menas. Av rent systematiska skäl verkar det vara kopplat till att verksamheten ska kunna omfattas av lagen oavsett hur stora de är. Den föreslagna formuleringen öppnar dock upp för att regeringen ganska fritt skulle utöka tillämpningsområdet och att även myndigheter skulle kunna ha den makten. Det är ganska riskfyllt och konsekvenserna av det kan bli stora. Överväg att formulera det ännu tydligare eller ta bort delegationen, jfr Certezzas förslag ovan.

Undantag från lagens tillämpningsområde
Sveriges säkerhet eller brottsbekämpning

Utredningens förslag	*Certezzas förslag*
11 § *Lagen gäller inte statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller brottsbekämpning.* *Regeringen får i föreskrifter ange vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.*	---

Skälen till Certezzas förslag:
Lagstiftaren eller regeringen bör inte i lag eller föreskrift peka ut verksamheter som till övervägande del bedriver säkerhetskänslig verksamhet. Vissa myndigheter kan en antagonist säkert räkna ut att de till övervägande del bedriver verksamhet som är av betydelse för Sveriges säkerhet, men som lagstiftaren har påpekat i förarbetena till säkerhetsskyddslagen, bör detta inte anges i lag eller föreskrift, jfr Certezzas synpunkter i anslutning till avsnitt 5.5.4 nedan. Det är rimligare att lagstiftaren direkt pekar ut de myndigheter som inte ska omfattas av regelverket utan hänvisning till säkerhetskänslighet eller brottsbekämpning. Certezza ifrågasätter dock varför brottsbekämpande myndigheter inte ska omfattas av regelverket.

Utredningens förslag	*Certezzas förslag*
12 § För *andra statliga myndigheter som utövar* säkerhetskänslig verksamhet *eller brottsbekämpning än de som avses i 11 §* gäller inte k*raven i 6 § andra och fjärde stycket samt kap. 3* för den del av verksamheten som är säkerhetskänslig *eller utgör brottsbekämpning*. För den övriga delen av verksamheten gäller lagen i dess helhet. *Vad som anförs i första stycket gäller även regioner och kommuner.*	**12 §** För *verksamhetsutövare som bedriver* säkerhetskänslig verksamhet gäller *inte lagen* för den del av verksamheten som är säkerhetskänslig. För den övriga delen av verksamheten gäller lagen i dess helhet.

Skälen till Certezzas förslag:
Certezza förslår en lagstiftningsteknik som inte leder till svårtillämpade undantag och undantag till undantag. Om lagstiftaren ändå vill använda denna lagstiftningsteknik borde ”andra statliga myndigheter” kunna bytas ut mot ”offentliga verksamhetsutövare” Den föreslagna lagtexten är näst intill obegripligt formulerad. Att statliga myn-

digheter, kommuner och regioner skulle vara gränsöverskridande verksamhetsutövare som då skulle slippa utse en företrädare förefaller något apart. Att de dessutom skulle slippa kraven i 6 § fjärde stycket får anses innebära att dessa inte riskerar ingripanden eller sanktioner enligt 5 kap. I avsnitt 5.5.4 resonerar dock utredningen för att verksamheterna skulle undantas från ”*kravet på incidentrapportering, riskhanteringsåtgärder och kravet om att utse en företrädare samt tillsyn och sanktioner som hänför sig till dessa krav*.” (s. 165 i betänkandet). Om lagstiftaren använder denna lagstiftningsmodell föreslår Certezza att den skrivs tydligare. T.ex. kan det i lagtexten stå ”*För den del av verksamheten som är säkerhetskänslig eller rör brottsbekämpning gäller inte 3–5 kap. Gränsöverskridande verksamhetsutövare behöver inte utse företrädare för den del av verksamheten som är säkerhetskänslig eller rör brottsbekämpning*.”

Nu anser emellertid Certezza att lagstiftaren bör överväga en annan teknik som är betydligt enklare och som leder till ett bättre resultat. Certezza anser att 11 § ska tas bort, se skäl ovan och även 13 § tas bort och det bör räcka med att undanta säkerhetskänslig verksamhet såsom Certezza föreslagit i paragrafen. Om en verksamhetsutövare bedriver verksamhet som är både säkerhetskänslig och inte säkerhetskänslig så gäller lagen fullt ut på den icke säkerhetskänsliga delen och tillsyn och sanktioner bör kunna träffa den delen.

Utredningens förslag	*Certezzas förslag*
13 § *Lagen gäller inte för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller som enbart erbjuder tjänster till statliga myndigheter som avses i 11 §.* *Om en enskild verksamhetsutövare bedriver även annan verksamhet gäller för den säkerhetskänsliga verksamheten, brottsbekämpningen och verksamheten som avser tjänster till statliga myndigheter enligt 11 § inte kraven i 6 § andra och fjärde stycket samt kap. 3. För den övriga delen av verksamheten gäller lagen i dess helhet.* *Vad som anförs ovan i andra stycket gäller inte om verksamhetsutövaren är en tillhandahållare av betrodda tjänster. För dessa verksamhetsutövare gäller lagen i dess helhet.*	---

Skälen till Certezzas förslag:
Bestämmelsen kan tas bort då det kan hanteras med det förslag som Certezza lämnar i anslutning till 12 § ovan, se skälen till Certezzas förslag i anslutning till den paragrafen.

Utredningens förslag	*Certezzas förslag*
2 kap. ***Klassificering och registrering***	**2 kap.** ***Väsentliga och viktiga verksamhetsutövare***
1 § Följande verksamhetsutövare är väsentliga: 1. Statliga myndigheter, 2. Verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet*, är en kommun eller ett lärosäte med examenstillstånd* och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1-3 i bilagan till kommissionens rekommendation 2003/361/EG, 3. […]	**1 §** Följande verksamhetsutövare är väsentliga: 1. Statliga, *regionala och kommunala myndigheter,* 2. *Enskilda v*erksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1-3 i bilagan till kommissionens rekommendation 2003/361/EG, 3. *Lärosäten med examenstillstånd vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1-3 i bilagan till kommissionens rekommendation 2003/361/EG.* 4. […]

Skälen till Certezzas förslag:
Andra kapitlet består av endast två paragrafer. Överväg att inkludera bestämmelserna i ett andra kapitel, särskilt eftersom Certezza föreslår att bestämmelsen om registrering flyttas till 1 kap. se nedan. Begreppet klassificering är olyckligt i sammanhanget. Andra regelverk innehåller begreppet klassificering, exempelvis säkerhetsskyddslagen och arkivlagen.

När det sedan gäller själva lagtexten så blir den tyvärr förvirrande och missvisande. Utredningen konstaterar i avsnitt 6.1, (s. 174 i betänkandet) att alla kommuner är väsentliga då borde det vara bättre att ange det i samband med statliga myndigheter eller ange det i en egen punkt. Det kan också vara klokt att i sådant fall även ange att det är kommunala myndigheter som aves. Begreppet ”är en kommun” förefaller något oprecist i sammanhanget.

För att undvika syftningsproblem kan det vara klokt att ange lärosäten med examenstillstånd i en egen punkt. Certezza tror att lagstiftningen skulle tjäna på att vara tydligare enligt vårt förlag.

Utredningens förslag	*Certezzas förslag*
2 § *Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Gränsöverskridande verksamhetsutövare ska även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren.* *Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.* Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om *uppgifterna*.	**1 kap. Inledande bestämmelser** ***9 §*** *Alla enskilda verksamhetsutövare som omfattas av lagen ska anmäla verksamheten till tillsynsmyndigheten.* Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om *vilka uppgifter som ska lämnas till tillsynsmyndigheten i anmälan och när anmälan ska göras efter att verksamhetsutövaren ändrat uppgifterna som ska anmälas till tillsynsmyndigheten.* Gränsöverskridande verksamhetsutövare ska alltid lämna uppgift till *tillsynsmyndigheten* om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren. *Tillsynsmyndigheten ska lämna uppgift till den myndighet som regeringen bestämmer om gränsöverskridande verksamhetsutövare.*

Skälen till Certezzas förslag:
Bestämmelsen bör flyttas till kapitel 1. Eftersom alla som omfattas av lagen också har en skyldighet att anmäla verksamheten till tillsynsmyndigheten. Därför bör anmälan snarare vara kopplad till huruvida verksamhetsutövaren träffas eller inte träffas av lagstiftningen än huruvida verksamhetsutövaren är en väsentlig eller viktig aktör. Offentliga verksamhetsutövare bör vara kända för tillsynsmyndigheten genom lagstiftningen såsom den föreslås och borde därför kunna slippa anmälningskravet.

Innehållet i anmälan bör också till största delen kunna hanteras inom ramen för föreskrifter av tillsynsmyndigheten. Tillsynsmyndigheten har i allmänhet störst kännedom om vilka uppgifter som de behöver för att kunna bedriva tillsyn något som skulle kunna vara olika beroende på vilken sektor som är aktuell. När det t.ex. kommer till IP-adressintervall tillämpar många aktörer dynamiska IP-adresser därför kan det bli märkligt att föreskriva detta i en lag, för att hantera bristen på IPv4 adresser tillämpar många tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, så kallade NAT-adresser, vilket innebär att en verksamhetsutövare som köper in kommunikationstjänster från sådana operatörer kanske inte ens har en egen IP-adress eller har det endast för vissa av tjänsterna. Det är oklart om även sådana så kallade NAT-adresser ska anmälas. Bestämmelsen skulle kunna kondenseras betydligt.

Sista stycket om delegation av föreskriftsrätt är ofullständigt och behöver förtydligas.

Tidsfristen för anmälan av ändringar skulle kunna hanteras av tillsynsmyndigheten baserat på deras egna interna processer och behoven inom sektorn.

Utredningens förslag

3 kap. *Riskhanteringsåtgärder* och incidentrapportering

1 § Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska *riskhantering*såtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska *utgå från ett allriskperspektiv och en riskanalys* och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande:

1. incidenthantering,
2. kontinuitetshantering
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. *strategier och förfaranden för användning av kryptografi och kryptering,*
6. personalsäkerhet
7. *strategier för åtkomstkontroll och tillgångsförvaltning,*
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om *riskhantering*såtgärder.

Certezzas förslag

3 kap. *Säkerhetsåtgärder* och incidentrapportering

1 § Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska *säkerhets*åtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna *ska dokumenteras i en riskanalys och* beakta *alla relevanta risker. Åtgärderna ska* vara *lämpliga och* proportionella i förhållande till risken. De ska *dokumenteras*, utvärderas och särskilt innefatta följande:

1. *strategier och förfaranden för*
   a. *riskanalys och informationssystemens säkerhet*
   b. *att bedöma effektiviteten i säkerhetsåtgärderna för cybersäkerhet,*
   c. *användning av kryptografi och, när så är lämpligt, kryptering,*
   d. *åtkomstkontroll och tillgångsförvaltning,*
2. incidenthantering,
3. kontinuitetshantering
4. säkerhet i leveranskedjan,
5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
6. *grundläggande praxis för cyberhygien*,
7. personalsäkerhet
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering

Regeringen eller den myndigheten regeringen bestämmer får meddela föreskrifter om *säkerhets*åtgärder.

Skälen till Certezzas förslag:
Certezza anser att lagstiftningen bör ansluta sig till etablerat svenskt språkbruk, använd säkerhetsåtgärder istället för riskhanteringsåtgärder.

Utredningen har valt att inte inkludera rekvisitet ”lämpliga”. Certezza anser att det är ett viktigt rekvisit som anknyter till de särskilda förutsättningar som varje verksamhetsutövare har. Det är viktigt för verksamhetsutövare att i förhållande till tillsynsmyndigheten kunna invända att en viss åtgärd inte är lämplig trots att det skulle vara proportionellt att ställa krav på den. I sådant fall bör verksamhetsutövaren inte vara skyldig att införa den påbjudna åtgärden.

Utredningen har inte tagit med vissa säkerhetsåtgärder såsom strategier för riskanalys och informationssystemens säkerhet, bedömning av effektiviteten i säkerhetsåtgärderna samt grundläggande cyberhygien. Certezza anser att detta är åtgärder som bör finnas med i lagtexten. Det bör även kopplas ett dokumentationskrav avseende säkerhetsåtgärderna. Om verksamhetsutövaren inte dokumenterar åtgärderna kommer de bara att finnas i huvudet hos befattningshavare. Det är varken lämpligt eller möjligt för tillsynsmyndigheten att kontrollera, se vidare avsnitt 7.1.2 nedan.

5 kap. Ingripanden och sanktioner

Utredningens förslag	*Certezzas förslag*
5 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren […] 4. har *hindrat* säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller […]	**5 §** En överträdelse ska betraktas som allvarlig om verksamhetsutövaren […] 4. *har försvårat eller utan giltigt skäl försenat* säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller […]

Skälen till Certezzas förslag:
Att hindra säkerhetsåtgärder eller tillsynsåtgärder torde vara mycket ovanligt och svårt att leda i bevis. Däremot är det inte otänkbart att tillsynsobjekt på olika sätt obstruerar vid tillsyn eller oskäligen vill skjuta tillsynsåtgärder eller revisioner framför sig, kanske för att verksamhetsutövaren inte har alla åtgärder på plats som den borde och vill köpa sig tid för att undvika sanktioner, se även avsnitt 9.4.2, (s. 263 i betänkandet).

Förbud att utöva ledningsfunktion

Utredningens förslag	*Certezzas förslag*
8 § Om ett föreläggande enligt 6 § inte följts får *tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker* hos allmän förvaltningsdomstol om att *en person* inte ska få *vara befattningshavare hos en viss verksamhetsutövare* (förbud). […]	**8 §** Om ett föreläggande enligt 6 § inte följs får tillsynsmyndigheten ansöka hos allmän förvaltningsdomstol om att befattningshavare *hos en viss verksamhetsutövare* inte ska få utöva *ledningsansvar* (förbud). […]

Skälen till Certezzas förslag:
Bestämmelsen skulle kunna skrivas på ett enklare sätt.

Det kan vara fler än en befattningshavare som tillsammans och i samförstånd inte följer föreläggande, därför bör sanktionen inte vara begränsad till en (1) person. Det bör även förtydligas att det är just befattningen med ledningsansvar som man inte får ha. Personen eller personerna i fråga kan ha andra befattningar som de så klart borde fortsätta att kunna ha hos verksamhetsutövaren, till exempel sköta utbetalningar med mera. Begreppet ledningsansvar skulle behöva förtydligas, se avsnitt 9.5.6, (s. 278 f. i betänkandet).

Utredningens förslag	*Certezzas förslag*
9 § Ett beslut om förbud enligt 8 § fattas av förvaltningsrätten *på* ansökan *från* tillsynsmyndigheten. En ansökan ska innehålla uppgifter om 1. den person som ansökan avser […]	**9 §** Ett beslut om förbud enligt 8 § fattas av förvaltningsrätten *efter* ansökan *av* tillsynsmyndigheten. En ansökan ska innehålla uppgifter om 1. den *eller de* person*er* som ansökan avser *och uppgift om den eller de befattningar som ansökan avser*, […]

Skälen till Certezzas förslag:
Som Certezza nämnt ovan bör förvaltningsdomstolarna kunna hantera flera befattningshavare i samma ansökan. Det kan också vara relevant för förvaltningsdomstolarna att redan i ansökan få kännedom om vilken befattning som personerna har hos verksamhetsutövaren.

4.6 Förvaltning av IKT-tjänster mellan företag

Den 22 december 2023 publicerades rättelse 2023/90206 till NIS 2-direktivet i Europeiska unionens officiella tidning.[2] Denna rättelse verkar ha förbigått utredningen och innebär en förändring i förhållande till de aktörer som ska omfattas av regelverket. Visserligen är NIS2-direktivet ett minimi-direktiv men som utredningen formulerat det innebär förslaget en utvidgning jämfört med hur artiklarna formuleras efter rättelsen. Utredningen har inte resonerat kring denna utvidgning av tillämpningsområdet.

Av rättelsen framgår bland annat att alla förekomster av ”leverantörer av hanterade tjänster” ska ersättas med ”leverantörer av utlokaliserade drifttjänster”, med nödvändiga anpassningar samt att alla förekomster av ”leverantör/leverantörer av hanterade säkerhetstjänster” ska ersättas med ”leverantör/leverantörer av utlokaliserade säkerhetstjänster”, med nödvändiga grammatiska anpassningar. Denna rättelse får inverkan på hur denna sektor omfattas av regelverket och behöver därför genomgående anpassas och förtydligas i det fortsatta lagstiftningsarbetet. Särskilt eftersom leverantör av utlokaliserade säkerhetstjänster kräver att aktören dessutom är en leverantör av utlokaliserade driftstjänster. Jfr definitionen av ”leverantör av utlokaliserade säkerhetstjänster: en leverantör av *utlokaliserade driftstjänster* som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker”, (vår kursivering).

Det skulle med andra ord utesluta oberoende rådgivningstjänster rörande säkerhetsåtgärder. Certezza anser att det är viktigt att lagstiftaren är tydlig med att utlokaliserade säkerhetstjänster är nödvändigt förknippade med aktör som tillhandahåller utlokaliserade driftstjänster.

5.2.2 Verksamhetsutövare

Certezza anser till skillnad från utredningen att verksamheterna som huvudregel inte ska ingå i sin helhet. Endast de delar av verksamheten som är av betydelse för att tillhandahålla de varor eller tjänster som direktivet är avsett att skydda bör ingå. Naturligtvis kommer många verksamheter i sin helhet ändå att omfattas eftersom de enbart är verksamma i en viss sektor eller verksamhet som omfattas av lagstiftningen. Men för de verksamhetsutövare som har verksamhet i flera sektorer kan det leda till att regelverket blir onödigt betungande. Utredningen påtalar gränsdragningsproblem med att dela upp verksamheten, men samtidigt anger utredningen i avsnitt 5.5.4 (s. 161 i betänkandet), att säkerhetskänsliga delar av verksamheterna kan undantas och verksamheten kan delas upp vid tillsyn. Utredningen resonerar också om att tillsynen skulle kunna delas upp i olika verksamhetsdelar, jfr avsnitt 8.4.7, (s. 242 i betänkandet).

[2] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202390206.

Även om det, som utredningen nämner, saknas en uttrycklig begränsning om att endast delar av den fysiska eller juridiska personens verksamhet omfattas av direktivet får det ändå av systematiska skäl och såsom bilagorna är utformade vara tydligt att det endast är de delar av verksamheten som omfattas av regelverket som ska skyddas och som har krav på säkerhets/riskhanteringsåtgärder. Att det kan finnas många system som är sammankopplade och att ett informationssystem som omfattas också används till andra verksamheter och därmed leder till högre säkerhet även för den verksamhet som inte omfattas torde endast vara en bonus för den oreglerade verksamheten. Men verksamhetsutövare borde inte riskera tillsynsåtgärder och sanktioner för delar av verksamheten som inte skulle ha omfattats av regelverket om man organiserat sin verksamhet på ett annat sätt. T.ex. skulle ett rent kontorssystem som inte har någon betydelse för tillhandahållande av en viss tjänst i en viss sektor inte behöva omfattas av regelverket. Men om det skulle ha betydelse för tillhandahållande av tjänsten så ska detta självklart också omfattas. Detta blir särskilt tydligt i förhållande till bland annat kommuner, se Certezzas synpunkter rörande avsnitt 5.2.10 Kommuner nedan. Därtill synes DORA-förordningen möjliggöra för olika krav för olika delar av verksamheterna vilket också starkt talar för att det är praktiskt möjligt att avskilja delar av verksamheterna som regelverket ska tillämpas på. Argumentet att det är svårt att dela upp verksamheter för att incidenter inom del av verksamheten kan få effekter för hela verksamheten visar bara på att en verksamhetsutövare som sammanblandat verksamheterna är extra sårbar. Har en verksamhetsutövare sammanblandat sin IKT-miljö på ett sådant sätt att det påverkar den del av verksamheten som omfattas av lagens regler är det naturligt att även sådant som annars inte skulle ha omfattats påverkas av regleringen. Tillämpar verksamhetsutövaren däremot segmentering och separering sin it-miljö – vilket är god cyberhygien – så är det lite som talar för de delarna som inte är högkritiska eller kritiska ska omfattas av regelverket. Utredningens förslag riskerar snarare att påverka verksamheter att inte segmentera eller separera sin it-miljö vilket kan öka sårbarheterna för verksamheten och tillhandahållande av tjänsterna. Ett system som däremot är integrerat med tillhandahållande av de högkritiska eller kritiska tjänsterna ska självklart omfattas dels eftersom det ökar sårbarheten för den kritiska verksamheten, dels riskerar att påverka tjänsterna. T.ex. skulle kommunala skolverksamheter it-tekniskt kunna avskiljas från kommunens övriga verksamhet och därmed inte behöva omfattas, se Certezzas synpunkter i avsnitt 5.2.10 nedan.

5.2.10 Kommuner

Certezza anser att det är viktigt höja nivån på cybersäkerheten i hela samhället och därför bör alla kommuner omfattas av regelverket på ett eller annat sätt, men Certezza anser att skälet, dvs att de flesta kommuner bedriver hemsjukvård och i fullständighetens namn ska även de som möjligtvis inte bedriver hemsjukvård omfattas, skulle behöva underbyggas mer. Mycket lämpligare vore att förtydliga att det är

kommunala myndigheter som omfattas samtidigt som det införs lämpliga undantag eftersom vissa kommunala verksamheter inte behöver omfattas.

Ett resultat av utredningens förslag blir att t.ex. kommunala skolhuvudmän omfattas av lagstiftningen samtidigt som privata skolhuvudmän inte omfattas av lagstiftningen. Det riskerar att skapa ännu mer ansträngda ekonomiska förutsättningar för skolorna eftersom efterlevnad av lagstiftningen är resurskrävande. Samtidigt kan privata skolalternativ använda sitt överskott till att fördela vinster till aktieägarna, det riskerar att snedvrida konkurrensen och påverka skolsystemet negativt. Redan idag är konkurrensen snedvriden då privata skolalternativ inte har samma krav på offentlighet och arkivföring något som är resurskrävande. För att slippa detta skulle kommunerna kunna knoppa av skolverksamheten och driva det som privata bolag men Certezza anser inte att det är lämpligt att införa ett regelverk som mer eller mindre skulle tvinga kommuner att bolagisera skolverksamheten enbart i syfte att undvika ett regelverk som de annars inte skulle omfattas av. Delar av skolans verksamhet kan ju också ifrågasättas det är så högkritiskt att det måste införas krav på sådana säkerhets/rikshanteringsåtgärder som regleras i 3 kap. i förslaget till ny cybersäkerhetslag. T.ex. kan skolverksamhet bedrivas även med fysiska medel såsom fysiska böcker, räkneböcker, katederundervisning, studiebesök, filmvisning med mera. Motsvarande resonemang kan föras även avseende andra kommunala verksamheter där det kan råda konkurrens med privata alternativ som inte omfattas av regelverket. Ett alternativ skulle kunna vara att även dessa verksamheter omfattas av cybersäkerhetslagen men den frågan har inte utretts.

Certezza ifrågasätter därför om det finns tillräckligt utredningsunderlag för att inkludera kommuner i tillämpningen av den nya cybersäkerhetslagen på det sätt som utredningen föreslår. Kommunala myndigheter utgör idag en stor och viktig del av den offentliga förvaltningen som medborgarna kommer i kontakt med idag. För att behålla medborgarnas förtroende för den kommunala förvaltningen är det en nödvändig förutsättning att kommunerna också satsar resurser på god cyberhygien och vidta säkerhets-/riskhanteringsåtgärder så att de kan undvika eller minska konsekvenserna av incidenter vilket kommer att bibehålla förtroendet.

Kommunerna är måltavlor för antagonistiska attacker och drabbas hårt av detta, jfr exempelvis cyberattackerna mot Bjurlöv kommun, Kalix kommun, Härjedalens kommun, Vellinge kommun, Falkenbergs kommun, Borgholms kommun, Kalmar kommun och Skånes Kommuner med flera, listan kan göras lång. Samtidigt har olika kommuner väldigt olika resurser och förutsättningar att tillhandahålla en tillräckligt hög nivå av cybersäkerhet. Här behöver staten bedriva ett såväl strategiskt som operativt arbete i att stötta kommunerna med resurser samt skapa ett regelverk som är lätt att tillämpa och som leder till att cybersäkerhetsnivån i hela Sverige kan höjas.

Förslag:

Regeringen bör omgående tillsätta en utredning med uppdrag att ta fram förslag på hur och i vilken omfattning kommunala och regionala myndigheter eller verksamheter ska omfattas av cybersäkerhetslagen samt lämna förslag på enkla kriterier att tillämpa för att bedöma om de kommunala och regionala verksamheterna är väsentliga eller viktiga.

5.5.4 Undantag för offentliga verksamhetsutövare

Generellt anser Certezza att det inte är lämpligt att i lagstiftning peka ut verksamheter som till övervägande del bedriver säkerhetskänslig verksamhet. Inte ens säkerhetsskyddslagen gör detta. Tvärtom ansåg lagstiftaren att det inte är en lämplig modell att peka ut vilka verksamheter som omfattas av säkerhetsskyddslagstiftningen.[3] En bättre modell vore att direkt i lagen peka ut vilka verksamheter som inte omfattas av lagen utan koppling till om verksamheten till övervägande del är säkerhetskänslig eller inte samt att undanta de delar av alla andra verksamheter som omfattas av säkerhetsskydd från lagens tillämpning.

Certezza ifrågasätter varför regeringen och Regeringskansliet ska undantas från regelverket. Certezza tycker att det sänder en viktig signal till samhället att regeringen och Regeringskansliet också underkastar sig kraven och föregår med gott exempel. Det är lätt att ställa krav på andra som man inte är villig att själv efterleva. Idag bedriver Riksrevisionen tillsyn över regeringen och Regeringskansliet och skulle kunna fortsätta bedriva tillsyn mot det aktuella regelverket för dessa myndigheter.

6.1 Väsentlig eller viktig

Se även skälen till Certezzas förslag i anslutning till lagtexten, avsnitt 1.1 ovan. Certezza föreslår att regeringen undviker ordet klassificering vid bedömningen av om en verksamhet är väsentlig eller viktig eftersom begreppet klassificering kan bli missvisande då det används för andra saker i näraliggande lagstiftning exempelvis säkerhetsskydds- och arkivlagstiftning samt i ISO-27000 standarden.

När det gäller frågan om en verksamhet är väsentlig eller viktig anser Certezza att det skulle vara bättre om det direkt framgår att regionala och kommunala myndigheter är väsentliga. Såsom utredningen har resonerat sig fram till och om lagstiftare delar det resonemanget.

Enligt artikel 2.2 f i NIS2-direktivet är statliga och regionala myndigheter undantagna från storlekskravet, trots de resonerar utredningen om detta beträffande regioner i avsnitt 5.2.9, (s. 134 i betänkandet). Enligt direktivet ska istället en riskbaserad bedömning göras i förhållande till regioner. Utredningen synes inte ha gjort en sådan riskbaserad bedömning, utan fokuserar enbart på regionernas storlek i förhållande till

[3] Prop. 2017/18:89 s. 43.

antalet anställda och omsättning. Det är möjligt att det är tillräckligt för att risken ska vara sådan att alla regioner ska omfattas. Men det skulle behövas ett utförligare resonemang kring den riskbedömning som ska göras. Utredningen har inkluderat kommuner som helhet i tillämpningsområdet för lagen och inte delat upp dem i myndigheter såsom utredningen gjort beträffande staten, därför hamnar kommunerna alltid över storlekskravet för att anse som väsentliga. Frågan är om det inte vore lämpligare att dela upp det på kommunala verksamheter eller myndigheter och att om verksamheten är viktig eller väsentlig får avgöras mot den bakgrunden. Då skulle kommunala verksamheter eller myndigheter snarare bli viktiga om de ens skulle omfattas. Samtidigt som vissa kommuners kommunala verksamheter skulle anses vara väsentliga.

För tydlighetens skull anser Certezza att de flesta kommunala myndigheter bör omfattas och att alla kommuner bör behandlas på ett likartat sätt. Certezza har i anslutning till avsnitt 5.2.10 föreslagit att regeringen tillsätter en utredning om kommuner och regioner ska omfattas. Denna utredning bör inkludera enkla kriterier för att fastställa om verksamheten är väsentlig eller viktig.

Lärosäten med examenstillstånd bör anges i en egen punkt för att undvika problem med syftning i bestämmelsen.

6.2 Register över väsentliga och viktiga verksamhetsutövare

Såsom Certezza framfört i anslutning till lagtexten i avsnitt 1.1 ovan, kommer registret inkludera såväl väsentliga som viktiga aktörer. Ingen verksamhet som omfattas av lagstiftningen är tänkt att falla utanför anmälningsplikten. Därför bör anmälningsplikten dispositionsmässigt höra till reglerna som anger om en verksamhet omfattas eller inte.

Certezza anser dessutom att innehållet i anmälan och hur snabbt anmälan vid förändringar måste lämnas bör anpassas till tillsynsmyndighetens behov och behöver inte anges i lag. Därför kan det räcka att tillsynsmyndigheten får meddela föreskrifter om vilka uppgifter som ska ingå i anmälan samt tidsfristen för anmälan av förändringar. Uppgifter om IP-adressintervall är många gånger inte vara relevant då det idag är ovanligt med fasta IP-adresser. Det har att göra med att antalet IPv4 adresser är begränsat. Något som också föranlett vissa verksamheter att använda alternativ till IP-adresser såsom exempelvis NAT-adresser för vissa tjänster. Dessa uppgifter är snarare något som kan lämnas vid behov i samband med tillsynsåtgärder.

Som utredningen föreslår ska den gemensamma kontaktpunkten (Myndigheten för samhällsskydd och beredskap, MSB), inte tillsynsmyndigheten, upprätta register över gränsöverskridande verksamhetsutövare. För att kunna göra det behöver således tillsynsmyndigheterna föra över sådana uppgifter till MSB alternativt att verksamhetsutövarna själva anmäler till MSB. Den mest lämpliga lösningen är dock att respektive tillsynsmyndighet informerar MSB om sådana verksamheter som anmälts till dem, det bör dock framgå av lagen.

7.1.1 Övergripande om begrepp

Certezza ansluter sig till MSB:s synpunkter i betänkandet om att begreppet säkerhetsåtgärder är det etablerade begreppet i svenskt språkbruk. Att man väljer att inkludera fler åtgärder är inget starkt skäl att frångå etablerat språkbruk. I dataskyddsförordningen och i DORA-förordningen tillämpas också begreppet säkerhetsåtgärder samtidigt som begreppet riskhantering används, dock inte i sammansättningen riskhanteringsåtgärder. Detta talar starkt för att begreppen säkerhetsåtgärder respektive riskhanteringsåtgärder får betraktas som synonymer ur ett EU-perspektiv. Certezza ser därför ingen särskild anledning att frångå etablerat svenskt språkbruk i detta sammanhang särskilt om det skulle få innebörden att riskhanteringsåtgärder på något sätt ska anses vara mer eller tyngre än begreppet säkerhetsåtgärder. Inom säkerhetsskyddslagen talar man om säkerhetsskyddsåtgärder. Möjligen skulle begreppet cybersäkerhetsåtgärder vara ett lämpligare ord om man vill använda något annat än säkerhetsåtgärder.

7.1.2 Riskhanteringsåtgärder

Utredningen har valt att utesluta rekvisitet ”lämpliga” med motiveringen att det är överflödigt eftersom det inte tillför något. Certezza delar inte slutsatsen att rekvisitet inte tillför något. Det kan tvärt om vara ett viktigt rekvisit som verksamhetsutövare kan använda visa för tillsynsmyndigheter eller domstol att en åtgärd som tillsynsmyndigheten föreslår eller förelägger faktiskt inte att lämplig att införa för verksamheten trots att åtgärden är proportionell. Rekvisitet bör därför inkluderas i den svenska lagtexten.

Utredningen föreslår bland annat att åtgärderna ska utgå från ett allriskperspektiv. Begreppet allriskperspektiv definieras inte eller förklaras av utredningen. Av direktivet antyds att allriskperspektiv också inkluderar fysiska risker. Certezza anser att det vore bättre att fokusera på relevanta risker vilket också inkluderar risker för den fysiska miljön och hot från insiders. I sammanhanget kan det vara värt att lyfta den kritik som framförts mot begreppet allriskperspektiv inom krisberedskapen. Allriskperspektiv uppfattas som att verksamhetsutövare ska ta höjd för alla risker som kan leda till att verksamheten påverkas. Att alltid överallt ta ställning till alla risker blir övermäktigt för de flesta aktörer.[4]

Certezza ser positivt på att riskanalys ska göras samtidigt är det viktigt att lyfta att det finns flera olika sätt att analysera risker, det vanligaste idag är s.k. kvalitativ riskanalys som resonerar kring sannolikheter men kvantitativ riskanalys är på frammarsch och leder många gånger till bättre och mer hållbara beslut för verksamheter. Det vore därför bra om regeringen i det fortsatta lagstiftningsarbetet utöver grad av

[4] Denward, C, Hedtjärn Swaling, V, Risk i svensk beredskap - En idéskrift om grundläggande problem och hur de kan lösas, FOI-R—5285—SE, 2022-11-17.

sannolikhet också resonerar kring kvantitativ och erfarenhetsbaserade riskbedömningar. Jfr. t.ex. FAIR-standarden eller CARVER-modellen för riskanalyser.

NIS2-direktivet räknar upp ett antal säkerhets-/riskhanteringsåtgärder men utredningen har valt att inte ta med alla i förslaget till lagstiftning. Utredningen menar att strategier för riskanalys och informationssystemens säkerhet inte behövs eftersom det följer av den övergripande regleringen. Certezza delar inte denna slutsats då sådana strategier är viktiga styrdokument för verksamheter. Av den övergripande regleringen framgår inte att dessa styrdokument ska finnas. Verksamheter som inte dokumenterar dessa strategier kommer således att ha en lucka i deras ledningssystem och strategin kommer att finnas i huvudet på någon tjänsteperson hos verksamhetsutövaren. Strategier för riskanalys och informationssystemens säkerhet bör således finnas med i punktlistan och det bör läggas till ett dokumentationskrav.

I punkten 2 om kontinuitetshantering bör det åtminstone läggas till i kommentaren ”återställning av säkerhetskopior” såsom vi har sett i den senaste TietoEvery-incidenten är erfarenheten att bara för att man har köpt säkerhetskopiering är det tydligen inte självklart att det ingår återställning av system från säkerhetskopior och att de återställda säkerhetskopiorna ska fungera.[5]

Punkten om strategier och förfaranden för att bedöma effektiviteten i riskhanterings-/säkerhetsåtgärderna för cybersäkerhet bör finnas med i lagen. Se kommentar ovan, Certezza delar inte uppfattningen att det följer av den övergripande regleringen. Krav på styrande dokument framgår inte av den övergripande regleringen. Det bör läggas till ett dokumentationskrav.

Motsvarande gäller punkten om grundläggande praxis för cyberhygien. Certezza tolkar detta snarare som ett handlingssätt som ska dokumenteras i verksamhetsutövarens ledningssystem, det är alltså inte något esoteriskt ändamål som följer av andemeningen i lagen utan Certezza ser det som nödvändiga åtgärder för att anställda hos verksamhetsutövarens ska veta hur de ska agera för att säkerställa en grundläggande nivå av cybersäkerhet hos verksamhetsutövaren. Det bör således anges i lagen eller på annat sätt förtydligas att verksamhetsutövarna ska ha detta på plats och det ska finnas dokumenterat hos verksamhetsutövaren.

7.2 Ansvar och utbildning - riskhanteringsåtgärder

Certezza undrar om utredningen har missförstått innebörden av artikel 21.4. Bestämmelsen tar sikte på när entiteten själv inser att den inte följer reglerna och att den då vidtar alla nödvändiga åtgärder. Dvs sådant som skulle kunna framkomma vid en egen intern säkerhetsrevision, egen säkerhetsgranskning eller liknande. Att vänta till dess tillsynsmyndigheten har inlett tillsyn kan inte anses tillräckligt. För att uppfylla kraven i direktivet bör det således snarare anses försvårande vid en tillsyn att verksamhetsutövaren känt till omständighet som visat att man inte uppfyller kraven och

[5] https://www.dn.se/sverige/tietoevry-efter-attacken-inga-brister-i-var-it-sakerhet/.

trots det inte agerat eller agerat för långsamt. Certezza håller alltså inte med utredningens slutsats om att artikeln uppfylls genom förslagen i kapitel 8 och 9.

Kravet att ledningsorgan godkänner och övervakar genomförandet av säkerhets-/riskhanteringsåtgärderna behöver anges i lagen. Det är enligt Certezzas mening inte tillräckligt att hänvisa till aktiebolagslagen. Särskilda och aktiva godkännanden i beträffande dessa specifika åtgärder är nödvändigt för såväl ansvarighet som för att säkerställa att ledningsorganen verkligen förstår vad de godkänner. Att övergripande hänvisa till andra ansvarighetsregler missar målet och kommer inte att leda till att cybersäkerhetsnivån i samhället höjs.

När det gäller utbildning anser Certezza att det inte räcker med en generell utbildning. NIS2-direktivet ställer krav på att den ska leda till tillräcklig kompetens för att kunna identifiera risker, bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av verksamhetsutövaren. Det innebär i stor utsträckning skräddarsydda utbildningar med kvalitetskrav – dvs. utbildning som ska leda till kompetens och bedömningsförmåga. Det räcker således inte att ledningen genom en utbildning enbart blir informerad. Detta behöver förtydligas i lag eftersom alla tillsynsmyndigheter säkerligen inte kommer att ställa sådana krav på utbildningen i deras respektive föreskrifter om de ens kommer att ställa några krav. Att **inte** införa kvalitetskrav på utbildningen i lagen uppfyller således inte direktivets krav.

7.3 Incidentrapportering

Certezza undrar över skälet att ha alla definitioner utom denna i 1 kap. och undrar om inte denna definition systematiskt hör hemma under avsnittet *Uttryck i lagen*.

8.4.1 System för tillsyn

Certezza är medveten om att det ligger utanför utredningens uppdrag att samla tillsynsansvaret i en eller ett fåtal myndigheter. Men menar att det är dags för regeringen att släppa sargen och utreda detta i en särskild ordning. Utredningen uttrycker oro för att det skulle bli en mycket omfattande uppgift för en myndighet att utöva tillsyn över samtliga verksamhetsutövare. Det skulle dock kunna jämföras med Integritetsskyddsmyndigheten som är ensam tillsynsmyndighet över samtliga personuppgiftsansvariga i Sverige. Fördelarna men en eller några få centrala tillsynsmyndigheter skulle vara att

- myndigheten/erna får ett tydligt och fokuserat uppdrag,
- myndigheten/erna kan vid behov hämta stöd från sektorsmyndigheter,
- det eliminerar risken för överlappande och inkonsekvent tillsyn i situationer där en verksamhetsutövare är verksam i flera sektorer,
- mer enhetliga och tydliga myndighetsföreskrifter,
- det underlättar verksamhetsutövarnas kontakt med tillsynsmyndigheten,
- mer enhetlig och samlad praxis rörande tillsynen, och

- myndigheten/erna kan lämna en samlad bild till regeringen om efterlevnaden av regelverket.

Nackdelarna med att ha så många tillsynsmyndigheter som utredningen föreslår är att

- en mängd olika tillsynsmyndigheter som tillämpar olika metoder, arbetssätt, mätning av statistik m.m. kan påverka värdet av och möjligheten till jämförelser mellan sektorer. Viktiga data om förhållandena hos de olika verksamheterna på en aggregerad nivå riskerar därmed att gå förlorad,
- överhängande risk för överlappande och dåligt samordnad tillsyn,
- mängder av olika cybersäkerhetsregleringar som endast skiljer sig åt i mindre avseenden, och
- spretig och svårtillgänglig praxis.

Att nuvarande tillsynsmyndigheter har byggt upp kunskap är bra. Sverige behöver dock bygga upp ännu mer kunskap. Dessutom kan sektorsmyndigheterna med sin uppbyggda kunskap utgöra ett stöd vid tillsynsmyndighetens/ernas tillsyn. Utredningen pekar dessutom på konkurrens på arbetsmarknaden som en utmaning när alltför många myndigheter ska rekrytera sådan kompetens och bygga upp en organisation för att bedriva tillsyn. Detta skulle också kunna undvikas genom en eller några få centrala tillsynsmyndigheter. Det bästa, enligt Certezza, vore att inrätta en ny specialiserad statlig myndighet för tillsyn med uppgift att bedriva tillsyn över samtliga sektorer med undantag för vissa statliga myndigheter såsom, myndigheterna under riksdagen, regeringen, Regeringskansliet, utlandsmyndigheterna, myndigheter under försvarsdepartementet och Säkerhetspolisen. Försvarsmakten skulle kunna vara tillsynsmyndighet för myndigheter under försvarsdepartementet och Riksrevisionen skulle kunna vara tillsynsmyndighet för myndigheter under riksdagen, regeringen, Regeringskansliet, Försvarsmakten och Säkerhetspolisen. Ett alternativ skulle vara att ansluta sig till säkerhetsskyddslagens tillsynsmodell så mycket som möjligt och inrätta en (1) särskild tillsynsmyndighet för kvarvarande sektorer. Ett ytterligare alternativ till att inrätta en helt ny myndighet skulle kunna var att Nationella cybersäkerhetscentret får tillsynsuppgiften.

Förslag:

Regeringen bör omgående tillsätta en utredning med uppgiften att se över systemet för tillsyn enligt den nya cybersäkerhetslagen med inriktningen att tillsynen ska bedrivas av en eller några få myndigheter. Med inriktningen att en nyinrättad myndighet bedriver tillsyn över alla sektorer med undantag för vissa statliga myndigheter såsom, myndigheterna under riksdagen, regeringen, Regeringskansliet, utlandsmyn-

digheterna, myndigheter under försvarsdepartementet och Säkerhetspolisen. Försvarsmakten skulle kunna vara tillsynsmyndighet för myndigheter under försvarsdepartementet och Riksrevisionen skulle kunna vara tillsynsmyndighet för myndigheter under riksdagen, regeringen, Regeringskansliet, Försvarsmakten och Säkerhetspolisen.

8.4.2 Tillsynsmyndigheter i Sverige

Energi

Certezza förstår ambitionen att inte öka antalet tillsynsmyndigheter i onödan men undrar om inte Affärsverket Svenska Kraftnät vore lämpligare än Energimyndigheten att bedriva tillsyn över verksamhetsutövare inom el-sektorn och att Energimyndigheten kan fortsätta vara tillsynsmyndighet över sektorerna fjärrvärme, gas, olje- och drivmedelsförsörjning. På så sätt linjerar det bättre med tillsynssystemet inom säkerhetsskydd. Någon konkurrens mellan myndigheterna om kompetens torde inte i detta fall föreligga eftersom Affärsverket Svenska Kraftnät redan torde ha kompetensen inom ramen för sin tillsyn över säkerhetsskyddsregelverket.

Offentlig förvaltning

Certezza ifrågasätter modellen att de utpekade regionerna ska vara tillsynsmyndighet för varandra och över tillsynsmyndigheter inom sitt område och anser att det vore lämpligare att en myndighet som inte omfattas av lagstiftningen utför tillsynen över de som utövar tillsyn, exempelvis Säkerhetspolisen som redan idag utöver tillsyn över myndigheterna avseende säkerhetsskydd.

Avfallshantering, Tillverkning, produktion och distribution av kemikalier, tillverkning och forskning

För dessa sektorer föreslår utredningen att länsstyrelserna ska vara tillsynsmyndigheter och därigenom också ha mandat att meddela föreskrifter. Det bör övervägas om det är lämpligt att länsstyrelserna är tillsynsmyndigheter alternativt har föreskriftsmandat, se närmare i avsnitt 8.4.5 nedan.

8.4.5 Föreskrifter

Såsom nämnts ovan är förslaget att länsstyrelserna ska vara tillsynsmyndigheter över sektorerna avfallshantering; tillverkning, produktion och distribution av kemikalier; tillverkning samt forskning. Certezza anser inte att det är en lämplig modell att fyra olika myndigheter ska meddela föreskrifter inom samma sektorer beroende på var verksamheten är lokaliserad i Sverige. Jfr 35 § andra stycket i förslag till förordning om cybersäkerhet, (s. 63 i betänkandet). Konsekvensen av utredningens förslag blir att fyra olika tillsynsmyndigheter ska meddela föreskrifter för samma sektorer. Det kan inte anses vara en ordning som skapar trygghet och ordning inom sektorerna.

Ska föreskrifterna endast ha regional räckvidd och hur ska de i sådant fall tillämpas på verksamhetsutövare som bedriver verksamhet i flera regioner? För offentlig förvaltning och lärosäten med examenstillstånd har utredningen föreslagit att MSB ska ha föreskriftsrätt avseende riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning antagligen för att undvika denna olyckliga omständighet. Men för ovan nämnda sektorer finns inte motsvarande förslag till undantag.

8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

Utredningen föreslår ett undantag för tillsynsmyndighetens tillträdesrätt till bostäder av integritetsskäl. Certezza anser att det finns en risk att de som är intresserade av att undvika tillsyn kommer att förlägga viss verksamhet i bostäder eftersom de vet att tillsynsmyndigheten inte kan komma åt verksamheten där. Utan detta undantag skulle det inte finnas något incitament för en verksamhetsutövare att bedriva verksamhet i privatbostäder och då skulle det inte heller finnas anledning att begära tillträde till bostäder. Om en tillsynsmyndighet skulle kräva tillträde till en bostad för tillsynsåtgärder så torde det finnas goda skäl till det. Utredningen har hänvisat till integritetsskäl som motiv till undantaget, men den verksamhetsutövare som förlägger verksamhet i sin privata bostad kanske inte har högt ställda krav på sin integritet. Certezza anser att vikten av att kunna kontrollera verksamheter fullständigt bör inbegripa rätten till tillträde till alla platser som verksamhetsutövaren har förlagt verksamhet, oavsett om det förlagts till en bostad eller inte.

8.4.7 Samordning och informationsutbyte

Verksamhetsutövare som står under tillsyn av flera myndigheter

Certezza anser att det är viktigt att en verksamhetsutövare inte drabbas onödigt hårt eller av motstridiga krav i samband med tillsyn. I detta fall föreslår utredningen en modell som innebär att tillsynsmyndigheterna endast ska bedriva tillsyn av del av verksamheten. Samtidigt har utredningen understrukit att det inte går att dela upp verksamheter, jfr avsnitt 5.2.2. Detta uppfattar Certezza som motsägelsefullt. Om det är möjligt att dela upp tillsynen borde det även vara möjligt att dela upp verksamheterna. Utredningen föreslår ingen konkret lösning på detta utan förutsätter att tillsynsmyndigheterna samarbetar vid genomförande av tillsyn rörande verksamhetsutövare som bedriver verksamhet i flera sektorer. Såsom Riksrevisionen har framfört verkar emellertid samordningen inom staten lämna en del att önska.[6] Certezza skulle därför vilja se en tydligare reglering för att lösa dessa situationer. Denna problematik skulle kunna lösas med en eller några få tillsynsmyndigheter, i enlighet med Certezzas förslag i avsnitt 8.4.1 ovan.

[6] Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig, (RiR 2023:8).

9.5.6 Förbud att utöva ledningsfunktion

Särskilda förutsättningar för att sanktionen ska komma i fråga

Som Certezza framfört i anslutning till Certezzas förslag om ändring av lagtexten, avsnitt 1.1 ovan, förefaller det märkligt att endast en (1) person i verksamhetens ledning ska kunna bli föremål för sanktionen. Bestämmelsen borde inte vara avgränsad på det sättet. Även ledningsfunktionärer som tillsammans och i samförstånd inte följer förelägganden bör kunna förbjudas att utöva ledningsfunktionen. Även om sanktionen blir personligen riktad till varje enskild funktionär borde inte tillsynsmyndigheten vara begränsad till att ansöka om förbud för enbart en person och det bör kunna hanteras inom ramen för samma ärende hos förvaltningsrätten.

14.1 Förslaget till lag om cybersäkerhet

3 kap. Riskhanteringsåtgärder och incidentrapportering

Det bör förtydligas i kommentaren att kontinuitetshantering också inbegriper fungerande återställning av säkerhetskopior. Som Certezza framhållit i anslutning till avsnitt 7.1.2. ovan, anser inte alla driftsleverantörer att begreppet säkerhetskopiering inbegriper att säkerhetskopian ska kunna återskapa ett tidigare ”oskadat” läge med mindre än att man köper en särskild tilläggstjänst. Många köpare av tjänster för säkerhetskopiering förutsätter att en säkerhetskopia ska kunna återställa data efter en incident. Eftersom det idag inte verkar råda konsensus mellan driftsleverantörer och verksamhetsutövare är det tyvärr nödvändigt att förtydliga att i begreppet kontinuitetshantering ingår också att kunna återställa säkerhetskopior på ett fungerande sätt. I praktiken så innebär det att driftsleverantörer som tillhandahåller säkerhetskopiering också måste säkerställa att säkerhetskopiorna kan återställas för kunderna.