

Justitiedepartementet

Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)
Remiss från justitiedepartementet.

Ert Dnr Ju2017/03997/L4

Sammanfattning

Utredningen uppfattas som ett mycket omfattande material som det är svårt att ta till sig i detalj, å andra sidan finns det även detaljer som vid ett flertal tillfällen återkommer ur olika perspektiv, vilket ibland gör det svårt att hålla isär de olika områdena och vad som avses. Materialet känns dock genomarbetat och väl-förankrat med en tydlig strategi och struktur, där samtliga ansvarsområden har en tydlig ansvars- och uppföljningsstruktur.

Det ligger i kommuners och leverantörers av kommunala tjänsters intresse att sektorerna som omnämns i utredningen fungerar på ett robust sätt. Dock är det svårt att ur utredningen överblicka vilka resurser som kommer krävas av kommunerna för att uppnå önskat resultat. Beroende på kommunstorlek kommer det sannolikt krävas olika mycket resurser. Även eventuella sanktionsavgifter kan slå olika på kommuner beroende på kommunstorlek. Kommuner organiserar sin verksamhet utifrån de intäkter som genereras i kommunen och de förutsättningar och kompetenser som finns i respektive kommun. Förutsättningarna för att implementera ny lagstiftning lyckosamt, om det innebär att ytterligare resurser behöver tas i anspråk, gynnas snarare av att medel följer med ut till kommunerna än att de drabbas av sanktionsavgifter.

Kommunerna kan komma långt i implementeringsarbetet inom ramen för sina befintliga RSA-arbeten men behövs det gå mycket längre är det angeläget att tillskjuta resurser till kommunerna för detta.

Östhammars kommun har också inhämtat synpunkter från vår VA-leverantör, Gästrike Vatten (GVAB) för att belysa utredningen ur deras perspektiv:

Generellt

- GVAB är generellt positiva till ökade krav på informationssäkerhet för samhällsviktiga och digitala tjänster
- GVAB ser generellt ökade kostnader för VA-huvudmannen genom ökade investeringsbehov (omfattningen beror på om kan vi komplettera befint-

ligt system eller måste vi köpa nytt) samt behov av kompetensförsörjning.

Krisberedskap

- MSB's krisberedskap behöver stärkas för att säkra vattenförsörjningen.
- Säkerhetsklassning på fler nivåer (utifrån rikets säkerhet) än vad som är möjligt idag.
- GVAB stödjer att VAKA ska finnas kvar som krisberedskapsstöd. Det finns en vinst med att VAKA verkar övergripande med en samlad kompetens för att stödja olika delar inom kommuner, länsstyrelser och myndigheter.

Sekretess

GVAB anser att det är viktigt att minska risken för att känsliga uppgifter sprids till obehöriga genom att tillsynsmyndigheten inte i onödan begär ut sekretessbelagda uppgifter. GVAB föreslår därför att det införs en rekommendation i den föreslagna lagen om att tillsynsmyndigheten vid tillsyn ska överväga vilka handlingar som begärs in och att tillsynsmyndigheten i den mån det är möjligt ska granska känsliga handlingar på plats. Den föreslagna rekommendationen stämmer väl överens med Livsmedelsverkets rekommendationer i "Vägledning till Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar" (se sidan 15 i vägledningen)."

Bakgrund

Utredningen utmynnar i ett författningsförslag som består av en lag och en förordning. Den nya lagen och förordningen ska vara åtgärderna som behövs för att implementera NIS-direktivet.

NIS-direktivet har bäring på en hög EU-gemensam nivå på säkerhet i nätverk och informationssystem, vilket innebär att medlemsstaterna ska

- anta en nationell strategi för säkerhet i nätverk och informationssystem,
- införa säkerhets- och incidentrapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster,
- utse nationella behöriga myndigheter, nationella kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och reglera samarbetet dem emellan,
- ingå i en samarbetsgrupp för strategiskt samarbete och informationsutbyte och
- ingå i ett nätverk för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverk).

samt

- identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium, och i det syftet
- upprätta en förteckning över tjänster som är viktiga för att upprätthålla kritisk samhälls- och/eller ekonomisk verksamhet.

Av de punkter som nämnts ovan berörs kommuner framför allt av införandet av säkerhets- och incidentrapportering, men också som leverantör av identifikation-

er på samhällsviktiga tjänster samt remissinstans för det fortsatta arbete tex med den nationella strategin.

De sektorer som ska omfattas av NIS-implementeringen är

- Transporter
- Hälsa- och sjukvård
- Leverans och distribution av dricksvatten
- Energi
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Digital infrastruktur och digitala tjänster

Kommuner kan påverkas som tillhandahållare av hälso- och sjukvård, leverans och distribution av dricksvatten, väghållare, energileverantör, bredbandsleverantör men har också beroenden till bankverksamhet (transaktioner av alla dess slag) och digitala infrastrukturen/tjänsterna (extern IT-kommunikation). En havererad finansmarknadsinfrastruktur skulle förr eller senare få svåra konsekvenser för kommuner.

Kommunerna kommer alltså att ha tre till fyra områden där det förväntas åtgärder och efterlevnad av vad NIS-implementerad författning säger. Där finns tre sektorer till där kommunerna inte är direkt berörda men där kommuner är, bland många andra aktörer, beroende av hög säkerhet och funktionalitet. Kommunerna kommer att ha tre till fyra olika statliga myndigheter som kontrollorgan för efterlevnaden av författningen. Därtill kan man tänka sig ytterligare en statlig myndighet som kommer att vara involverad utifrån risk- och sårbarhetsanalytiska dimensionen: MSB.

Merparten av det identifikationsarbete som kommer göras kommer sannolikt ske via kommunerna och det är önskvärt att så stor del av det kan ske inom ramen för befintligt RSA-arbete i kommunerna, där moment som exempelvis identifiera av kritiska beroenden och sårbarheter, arbeta systematiskt och riskbaserat med informationssäkerhet, förebygga händelser och minimera verkningar av oönskade händelser är moment som redan inkluderas i kommunernas RSA-arbete med olika ambitionsnivå beroende på kommunernas enskilda förutsättningar. Uppstyrning, harmoniseringar och utökningar är dock att förvänta till följd av NIS-implementeringen vilket kommer kräva mer resurser.

Helt nytt blir den incidentrapportering ska göras. Det innebär nya rutiner och nya arbetsmoment för kommuner. Vid incident kan kommunikation med allmänheten bli aktuellt.

Om kontrollorgan anser att en kommun inte lever upp till NIS-författningen, ska kommunen betala sanktionsavgift.