



## Informationssäkerhet för samhällsviktiga och digitala tjänster

---

### Sammanfattning

Utskottet ställer sig bakom regeringens förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster samt lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster.

I syfte att genomföra EU:s s.k. NIS-direktiv (dvs. direktivet om nät- och informationssäkerhet) i svensk rätt föreslås i propositionen en ny lag som bl.a. innebär att vissa leverantörer av samhällsviktiga och digitala tjänster ska vidta åtgärder till skydd för säkerheten i nätverk och informationssystem, att leverantörerna ska rapportera incidenter som påverkar kontinuiteten i tjänsterna och att den myndighet som regeringen bestämmer ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till den följs samt ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som inte följer lagens bestämmelser.

Regeringen föreslår att den nya lagen ska träda i kraft den 1 augusti 2018. Ändringen i den nya lagen med anledning av den nya säkerhetsskyddslagen föreslås träda i kraft den 1 april 2019.

Utskottet anser att riksdagen bör avslå motionsyrkandena.

I betänkandet finns fyra reservationer (KD, -) och ett särskilt yttrande (M, C, L, KD).

#### *Behandlade förslag*

Proposition 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster.

Sju yrkanden i följdmotioner.

# Innehållsförteckning

Utskottets förslag till riksdagsbeslut .....	3
Redogörelse för ärendet .....	5
Ärendet och dess beredning.....	5
Bakgrund .....	5
Propositionens huvudsakliga innehåll .....	6
Utskottets överväganden.....	7
Ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster .....	7
Reservationer .....	13
1. En ny cybersäkerhetsmyndighet, punkt 2 (KD).....	13
2. It-standardplattformar och en sammanhållen serviceorganisation, punkt 3 (-).....	13
3. Mikrosatellit teknik för säkra myndighetsnätverk, punkt 4 (-) .....	14
4. Säkerhetsklassad information och EU:s institutioner, punkt 5 (-) .....	15
Särskilt yttrande .....	16
Ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster, punkt 1 (M, C, L, KD) .....	16
<i>Bilaga 1</i>	
Förteckning över behandlade förslag .....	17
Propositionen .....	17
Följdmotionerna .....	17
<i>Bilaga 2</i>	
Regeringens lagförslag .....	18
1 Förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster .....	18
2 Förslag till lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster.....	25

# Utskottets förslag till riksdagsbeslut

## 1. Ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Riksdagen antar regeringens förslag till

1. lag om informationssäkerhet för samhällsviktiga och digitala tjänster,
2. lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Därmed bifaller riksdagen proposition 2017/18:205 punkterna 1 och 2.

## 2. En ny cybersäkerhetsmyndighet

Riksdagen avslår motion

2017/18:4139 av Andreas Carlson m.fl. (KD) yrkandena 1–4.

*Reservation 1 (KD)*

## 3. It-standardplattformar och en sammanhållen serviceorganisation

Riksdagen avslår motion

2017/18:4141 av Mikael Jansson m.fl. (-) yrkande 1.

*Reservation 2 (-)*

## 4. Mikrosatellit teknik för säkra myndighetsnätverk

Riksdagen avslår motion

2017/18:4141 av Mikael Jansson m.fl. (-) yrkande 2.

*Reservation 3 (-)*

## 5. Säkerhetsklassad information och EU:s institutioner

Riksdagen avslår motion

2017/18:4141 av Mikael Jansson m.fl. (-) yrkande 3.

*Reservation 4 (-)*

Stockholm den 31 maj 2018

På försvarsutskottets vägnar

*Allan Widman*

Följande ledamöter har deltagit i beslutet: Allan Widman (L), Åsa Lindestam (S), Hans Wallmark (M), Peter Jeppsson (S), Alexandra Völker (S), Mikael Jansson (-), Jan R Andersson (M), Kent Härstedt (S), Daniel Bäckström (C), Anders Schröder (MP), Lotta Olsson (M), Paula Holmqvist (S), Roger Richtoff (SD), Lotta Johnsson Fornarve (V), Mikael Oscarsson (KD) och Mattias Ottosson (S).

# Redogörelse för ärendet

## Ärendet och dess beredning

I juli 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, kallat NIS-direktivet. Medlemsstaterna skulle enligt direktivet senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att genomföra direktivet. Dessa bestämmelser skulle enligt direktivet tillämpas fr.o.m. den 10 maj 2018.

Regeringen beslutade i mars 2016 att ge en särskild utredare i uppdrag att föreslå hur NIS-direktivet ska genomföras i svensk rätt. I april 2017 överlämnade utredaren betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36).

Betänkandet har remitterats. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2017/03997/L4).

I den aktuella propositionen föreslås de lagändringar som bedöms vara nödvändiga för att genomföra NIS-direktivet i svensk rätt.

Regeringen har begärt in och i allt väsentligt följt Lagrådets synpunkter inför färdigställandet av propositionen. I förhållande till lagrådsremissen har också en författningsteknisk ändring och vissa språkliga och redaktionella ändringar gjorts i propositionen.

Två följdmotioner har väckts med anledning av propositionen.

Regeringsföreträdare från justitiedepartementet har löpande informerat utskottet om NIS-direktivets framväxt, t.ex. då den dåvarande statssekreteraren Ann Linde besökte försvarsutskottet den 3 december 2015. Statssekreterare Charlotte Svensson beskrev ansvarsfördelningen och samordningen inom informationssäkerhetsområdet för utskottet den 22 maj 2018.

## Bakgrund

Nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och för att EU:s inre marknad ska fungera.

Syftet med NIS-direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende och att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Flera av åtgärderna syftar mer specifikt till att säkerställa kontinuiteten i de samhällsviktiga och digitala tjänster som omfattas av direktivet.

## Propositionens huvudsakliga innehåll

I syfte att genomföra NIS-direktivet i svensk rätt föreslår regeringen en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster. Den nya lagen innebär bl.a. att

- vissa leverantörer av samhällsviktiga och digitala tjänster ska vidta åtgärder till skydd för säkerheten i nätverk och informationssystem
- leverantörerna ska rapportera incidenter som påverkar kontinuiteten i tjänsterna
- den myndighet som regeringen bestämmer ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till den följs, och den ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som inte följer lagens bestämmelser.

Regeringen föreslår att den nya lagen ska träda i kraft den 1 augusti 2018. Ändringen i den nya lagen med anledning den nya säkerhetsskyddslagen föreslås träda i kraft den 1 april 2019.

# Utskottets överväganden

## Ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster

### Utskottets förslag i korthet

Riksdagen antar regeringens förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster samt lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster. Samtliga motionsyrkanden avslås.

Jämför reservation 1 (KD), 2 (-), 3 (-) och 4 (-) samt det särskilda yttrandet (M, C, L, KD).

### Propositionen

I propositionen anger regeringen att NIS-direktivet i huvudsak ska genomföras genom en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster.

Syftet med den nya lagen är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för digitala tjänster samt för samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur.

Den nya lagen ska gälla för

- leverantörer av det slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst, under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (leverantörer av samhällsviktiga tjänster)
- juridiska personer som tillhandahåller en tjänst som utgör en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst och som har sitt huvudsakliga etableringsställe i Sverige eller som har utsett en företrädare som är etablerad här (leverantörer av digitala tjänster).

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som avses med en betydande störning vid tillhandahållandet av en samhällsviktig tjänst.

Den nya lagen ska inte gälla för

- vissa leverantörer av elektroniska kommunikationsnät och kommunikationstjänster
- vissa leverantörer av betrodda tjänster

- leverantörer av digitala tjänster som är mikroföretag eller små företag.

Regeringen anger vidare att den nya lagen inte ska gälla för säkerhetskänslig verksamhet.

I propositionen anger regeringen bl.a. att om det i en lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt den nya lagen.

För leverantörer av digitala tjänster får medlemsstaterna emellertid inte införa ytterligare säkerhets- eller rapporteringskrav, enligt direktivet.

I propositionen anges vidare att medlemsstaterna, för varje sektor som NIS-direktivet omfattar, ska identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium.

Förteckningen över samhällsviktiga tjänster ska senast den 9 november 2018 och därefter vartannat år tillhandahållas EU:s kommission som ett led i kommissionens arbete med att bedöma genomförandet av direktivet. Även information om antalet leverantörer som har identifierats i varje sektor och en uppgift om deras betydelse för sektorn ska inom samma tid lämnas till kommissionen.

Regeringen förslår därför att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vilka tjänster som utgör samhällsviktiga tjänster enligt den nya lagen.

I propositionen föreslås också att leverantörer av samhällsviktiga tjänster utan dröjsmål ska anmäla sig till tillsynsmyndigheten. Av en anmälan ska det framgå om leverantören tillhandahåller samhällsviktiga tjänster i två eller flera medlemsstater inom EU.

Regeringen anger i propositionen att leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete i fråga om de nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

Dessa leverantörer ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I analysen ska det ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

Leverantörerna ska vidare vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i de nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

Enligt propositionen ska leverantörer av samhällsviktiga tjänster också vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar de nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Regeringen eller den myndighet som regeringen bestämmer ska enligt propositionen få meddela föreskrifter om vad som krävs av leverantörer av samhällsviktiga tjänster för att de ska uppfylla kraven på säkerhetsåtgärder.



Leverantörerna ska enligt regeringens förslag rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller.

I den nya lagen ska det anges att incidentrapporteringen ska göras till den myndighet som regeringen bestämmer. Regeringen bedömer att incidentrapporteringen bör göras till den s.k. CSIRT-enheten (Computer Security Incident Response Team). Rapporteringen ska göras utan onödigt dröjsmål. Regeringen gör bedömningen att Myndigheten för samhällsskydd och beredskap (MSB) som utgångspunkt ska vara denna CSIRT-enhet.

Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet. Tillsynsmyndigheten ska utöva tillsyn över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs.

Med hänsyn särskilt till de skilda förhållanden som råder inom sektorerna och att förutsättningarna för en effektiv tillsyn förbättras om tillsynsmyndigheten har kunskap om den verksamhet som är föremål för tillsynen och om annan närliggande reglering, anser regeringen att utgångspunkten för tillsynens utformning bör vara att det ska finnas en tillsynsmyndighet för varje sektor.

Överträdelse av bestämmelser i den nya lagen bör inte vara straffsanktionerade, anger regeringen. Tillsynsmyndigheten ska enligt propositionen få meddela de förelägganden som behövs för att leverantörerna ska uppfylla kraven på utseende av företrädare, vissa säkerhetsåtgärder och incidentrapportering enligt den nya lagen och enligt föreskrifter som har meddelats i anslutning till lagen. Ett sådant föreläggande ska få förenas med vite.

En sanktionsavgift ska tas ut av den som underlåter att göra en anmälan till tillsynsmyndigheten, vidta vissa säkerhetsåtgärder eller incidentrapportera enligt den nya lagen eller föreskrifter som har meddelats i anslutning till denna, föreslår regeringen. Regeringen föreslår vidare att sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 10 miljoner kronor.

Regeringen bedömer att bestämmelser om vilken myndighet som ska vara nationell kontaktpunkt och vilka uppgifter som den nationella kontaktpunkten ska ha bör meddelas i förordning. Detsamma gäller för de bestämmelser om vilken myndighet som ska företräda Sverige i den samarbetsgrupp på EU-nivå som inrättats genom NIS-direktivet och de uppgifter som företrädaren ska ha. Utgångspunkten bör enligt regeringen vara att MSB ska ha rollen som nationell kontaktpunkt.

Regeringen föreslår avslutningsvis att den nya lagen ska träda i kraft den 1 augusti 2018. Ändringen i den nya lagen med anledning av den nya säkerhetsskyddslagen föreslås träda i kraft den 1 april 2019.

## **Motionerna**

Andreas Carlson m.fl. (KD) anför i motion 2017/18:4139 att den svenska cyber- och informationssäkerheten är i stort behov av förbättring. NIS-direktivet innebär att sådana steg har tagits på EU-nivå, och motionärerna är positiva till

detta. De delar regeringens uppfattning om att en ny lag krävs för att adekvata säkerhetsåtgärder ska kunna vidtas för att skydda säkerheten i nätverk och informationssystem m.m., men de delar däremot inte regeringens hållning att det är lämpligt att dela upp ansvaret på flera olika myndigheter. Enligt motionärerna leder det till en fragmentisering av systemet.

Motionärerna framför därför att en svensk cybersäkerhetsmyndighet bör inrättas (yrkande 1), att denna myndighet bör ges tillsynsansvar i frågor som gäller cyber- och informationssäkerhet (yrkande 2), att denna myndighet bör ges ett ansvar att ta fram de föreskrifter som ska styra svenskt cyber- och informationssäkerhetsarbete (yrkande 3) och att denna myndighet bör ges ett operativt ansvar för att implementera dessa föreskrifter (yrkande 4).

I motion 2017/18:4141 anför Mikael Jansson m.fl. (-) att Sverige kan vara mer ambitiöst än vad NIS-direktivet är på flera områden. Cybersäkerhet är ett svenskt nationellt säkerhetsintresse som dessutom kopplar an till utvecklandet av ett totalförsvaret, menar motionärerna.

I motionen framförs att staten, genom delar av totalförsvaret, bör tillhandahålla it-standardplattformar och en sammanhållen serviceorganisation för myndigheter med kritiska it-system (yrkande 1), att möjligheterna att använda svensk mikrosatellit teknik för att bygga säkra myndighetsnätverk bör utredas (yrkande 2) och att det bör säkerställas att säkerhetsklassad information av betydelse för svensk säkerhet inte automatiskt kommer EU:s institutioner till handa (yrkande 3).

### **Utskottets ställningstagande**

Då den nationella och internationella digitalisering som sker i dag går i hög fart och inte bara för med sig positiva möjligheter välkomnar utskottet det informationssäkerhetsarbete som regeringen bedriver, t.ex. genom den nyligen framtagna nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213, bet. 2017/18:FöU4, rskr. 2017/18:142) och den aktuella propositionen om informationssäkerhet för samhällsviktiga och digitala tjänster som motiveras av EU:s NIS-direktiv. Utskottet anser att det är nödvändigt med samarbete inom EU och internationellt för att främja informations- och cybersäkerheten eftersom den digitala utvecklingen är gränslös. Utskottet tillstyrker därför förslagen från regeringen på de skäl som anförs i propositionen.

Med anledning av det som förs fram i motion 2017/18:4139 (KD) yrkandena 1–4 vill utskottet lyfta fram vad Försvarsberedningen understryker i sin rapport Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025 (Ds 2017:66), bl.a. med anledning av NIS-direktivet, om vikten av att tillsyn och övervakning gällande informations- och cybersäkerhet i samtliga civila sektorer samordnas. De intentioner som regeringen uttrycker i propositionen i fråga om detta välkomnas därför av utskottet.

Utskottet vidhåller därmed det man uttryckte i betänkande 2017/18:FöU4, i fråga om de motionsyrkanden som där lades fram om en ny myndighet för cybersäkerhet, nämligen att arbetet med informationssäkerhet i grunden är ett

ansvar för hela samhället och alla aktörer. I enlighet med den vedertagna ansvarsprincipen bör berörda aktörer ansvara för att identifiera och möta informationspåverkan inom sina respektive ansvarsområden. Utskottet instämmer med vad regeringen uttryckte i strategin, dvs. att det i sammanhanget är särskilt viktigt med samverkan och en gemensam riktning för arbetet på området för att ingen kan lösa säkerhetsutmaningarna ensam. Även om den enskilda organisationen ytterst ansvarar för att hantera sin information är det i dagsläget enligt utskottet viktigt att förbättra förutsättningarna för att bedriva ett systematiskt och samordnat informationssäkerhetsarbete. Att skapa en för ändamålet särskild myndighet bedöms inte som kostnadseffektivt eller ändamålsenligt i dagsläget. Motion 2017/18:4139 (KD) yrkandena 1–4 avstyrks därmed.

Med anledning av motion 2017/18:4141 (-) vidhåller utskottet det man också uttryckte i betänkande 2017/18:FöU4 om att det är nödvändigt för att öka säkerheten i nätverk, produkter och system samt för att skapa en säker infrastruktur för elektronisk kommunikation att bl.a. verka för att elektroniska kommunikationsnät byggs på ett sådant sätt att de kan fungera oberoende av funktioner i andra länder. Aktörer inom allmän ordning, säkerhet, hälsa och försvar måste ha tillgång till moderna, säkra och robusta kommunikationslösningar. Utskottet har bl.a. i betänkande 2017/18:FöU6 också givit stöd åt regeringens intention att verka för ett effektivt cyberförsvar med förmågan att förebygga, upptäcka och hantera cyberangrepp, både för militär och för civil verksamhet.

Eftersom regeringen redan tidigare angett att strategin efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder på området för tillfället. Yrkandena i motion 2017/18:4141 (-) om att staten, genom delar av totalförsvaret, bör tillhandahålla it-standardplattformar och en sammanhållen serviceorganisation för myndigheter med kritiska it-system (yrkande 1) och om att möjligheterna att använda svensk mikrosatellit teknik för att bygga säkra myndighetsnätverk bör utredas (yrkande 2) avstyrks därmed.

När det gäller motion 2017/18:4141 (-) yrkande 3 vill utskottet avslutningsvis uttrycka att det delar regeringens bedömning att befintliga bestämmelser i offentlighets- och sekretesslagen tillgodoser NIS-direktivets krav på utlämnande av uppgifter till andra medlemsstater och till kommissionen. Detsamma gäller för kraven på skydd av uppgifter som mottagits från andra medlemsstater.

Utskottet har således inte någon annan uppfattning än regeringens, att sekretess inte utgör något hinder för informationsutbyte med andra medlemsstater och kommissionen enligt NIS-direktivet, den nya lagen eller föreskrifter i förordning som meddelats i anslutning till lagen. Något behov av ytterligare reglering i detta avseende bedöms inte finnas. Kommissionen, CSIRT-enheter och andra relevanta myndigheter har enligt NIS-direktivet en skyldighet att vid mellanstatligt informationsutbyte bevara informationens konfidentialitet och att skydda leverantörers säkerhetsintressen och kommersiella intressen.

Innan ett informationsutbyte sker måste det enligt regeringen dock beaktas att ett utlämnande av uppgifter inte får riskera Sveriges säkerhet. Regeringens förslag gäller enligt 8 § inte för verksamhet som omfattas av krav på säkerhetsskydd enligt den nu gällande säkerhetsskyddslagen (1996:627) och inte heller för den verksamhet som omfattas av den av riksdagen nyligen antagna nya säkerhetsskyddslagen som träder i kraft den 1 april 2019 (prop. 2017/18:89, bet. 2017/18:JuU21, rskr. 2017/18:289). Dessa bägge lagar gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet.

Härutöver kan påpekas att Sverige redan har ingått ett antal internationella överenskommelser om säkerhetsskydd, såväl bilaterala som multilaterala, med andra stater och internationella organisationer, bl.a. med EU.

Mot bakgrund av det anförda förutsätter utskottet att säkerhetsklassad information inte lämnas ut till EU:s institutioner utan att det först har prövats att så lagligen får ske. Motion 2017/18:4141 (-) yrkande 3 avstyrks därmed.

# Reservationer

## 1. En ny cybersäkerhetsmyndighet, punkt 2 (KD)

av Mikael Oscarsson (KD).

### *Förslag till riksdagsbeslut*

Jag anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion  
2017/18:4139 av Andreas Carlson m.fl. (KD) yrkandena 1–4.

### *Ställningstagande*

Jag menar att hoten mot den svenska cybersäkerheten vid det här laget torde vara välbekanta. Attackerna kan begås av kriminella, terrorister eller stater med en fientlig inställning gentemot Sverige. NIS-direktivet innebär att viktiga steg har tagits på EU-nivå för att stärka cybersäkerheten, och jag delar regeringens uppfattning om att en ny lag krävs för att adekvata säkerhetsåtgärder ska kunna vidtas.

Jag menar dock att regeringens förslag också innebär en fragmentering av det svenska arbetet med cybersäkerhet och att denna minskar vår förmåga att skydda oss mot de aktuella hoten. Cybersäkerhet är en expertkunskap, och den behöver samlas på en plats. Jag anser därför att en svensk cybersäkerhetsmyndighet bör inrättas, att myndigheten bör ges tillsynsansvar i frågor som gäller cyber- och informationssäkerhet, att myndigheten bör ges ett ansvar att ta fram de föreskrifter som ska styra svenskt cyber- och informationssäkerhetsarbete och att myndigheten bör ges ett operativt ansvar för att implementera dessa föreskrifter. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

## 2. It-standardplattformar och en sammanhållen serviceorganisation, punkt 3 (-)

av Mikael Jansson (-).

### *Förslag till riksdagsbeslut*

Jag anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion  
2017/18:4141 av Mikael Jansson m.fl. (-) yrkande 1.

### *Ställningstagande*

Jag anser att Sverige som land kan vara mer ambitiöst än vad NIS-direktivet är på flera områden. Cybersäkerhet är ett svenskt nationellt säkerhetsintresse som dessutom är nära förbundet med utvecklandet av ett totalförsvaret. I dagsläget använder myndigheterna olika it-plattformar och serviceorganisationer. Det gör att Sverige i ett totalförsvarsperspektiv saknar möjligheten att säkerställa en kontroll av myndigheternas it-säkerhet. Jag anser att staten, genom delar av totalförsvaret, bör tillhandahålla it-standardplattformar och en sammanhållen serviceorganisation för myndigheter med kritiska it-system. En myndighet som bygger it-plattformar och servicemallar åt de svenska myndigheterna bör ha anställda som är säkerhetsklassade svenska medborgare. Myndigheten bör inte utveckla teknik, det gör marknaden, men tekniken bör klassas och anpassas. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

### **3. Mikrosatellit teknik för säkra myndighetsnätverk, punkt 4 (-)**

av Mikael Jansson (-).

### *Förslag till riksdagsbeslut*

Jag anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion  
2017/18:4141 av Mikael Jansson m.fl. (-) yrkande 2.

### *Ställningstagande*

Jag anser att möjligheterna att använda svensk mikrosatellit teknik för att bygga säkra myndighetsnätverk bör utredas då cybersäkerhet är ett svenskt nationellt säkerhetsintresse. Jag anser således att Sverige som land kan vara mer ambitiöst än vad NIS-direktivet är på flera områden. Kostnadsdelning bör kunna sökas med de nordiska länderna. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

#### **4. Säkerhetsklassad information och EU:s institutioner, punkt 5 (-)**

av Mikael Jansson (-).

##### *Förslag till riksdagsbeslut*

Jag anser att förslaget till riksdagsbeslut under punkt 5 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion  
2017/18:4141 av Mikael Jansson m.fl. (-) yrkande 3.

##### *Ställningstagande*

Cybersäkerhet är ett svenskt nationellt säkerhetsintresse som dessutom är nära förbundet med utvecklandet av ett totalförsvar. Som ett militärt alliansfritt land bör vi inte okritiskt tillhandhålla vår säkerhetsklassade information till EU. Jag anser därför att det bör säkerställas att säkerhetsklassad information av betydelse för svensk säkerhet inte automatiskt kommer EU:s institutioner till handa. Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

## Särskilt yttrande

### **Ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster, punkt 1 (M, C, L, KD)**

Allan Widman (L), Hans Wallmark (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD) anför:

Vid regeringens information till utskottet angående ansvarsfördelningen inom statsförvaltningen i fråga om informations- och cybersäkerhetsfrågor framkom det att regeringen överväger olika alternativ för att stärka den nationella samordningen.

Arbetet med informations- och cybersäkerhet har under lång tid kritiserats av bl.a. Riksrevisionen. Det handlar om långsamhet vid implementeringen av befintliga regler och oklara ansvarsförhållanden. Med NIS-direktivets implementering tillkommer en rad nya myndigheter som får tillsynsuppgifter på området. Alliansen vill därför understryka vikten av att regeringen snabbt får en effektiv, nationell samordning på plats inom informations- och cybersäkerhetsområdet.



BILAGA 1

## Förteckning över behandlade förslag

## Propositionen

*Proposition 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster:*

1. Riksdagen antar regeringens förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster.

## Följdmotionerna

*2017/18:4139 av Andreas Carlson m.fl. (KD):*

1. Riksdagen ställer sig bakom det som anförs i motionen om att inrätta en svensk cybersäkerhetsmyndighet och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att ge denna myndighet tillsynsansvar i frågor som gäller cyber- och informationssäkerhet och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att ge denna myndighet ett ansvar att ta fram de föreskrifter som ska styra svenskt cyber- och informationssäkerhetsarbete och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att ge denna myndighet ett operativt ansvar för att implementera dessa föreskrifter och tillkännager detta för regeringen.

*2017/18:4141 av Mikael Jansson m.fl. (-):*

1. Riksdagen ställer sig bakom det som anförs i motionen om att staten genom delar av totalförsvaret bör tillhandahålla it-standardplattformar och en sammanhållen serviceorganisation för myndigheter med kritiska it-system och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att utreda möjligheterna att använda svensk mikrosatellit teknik för att bygga säkra myndighetsnätverk och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att säkerställa att säkerhetsklassad information av betydelse för svensk säkerhet inte per automatik kommer EU:s institutioner till handa och tillkännager detta för regeringen.

BILAGA 2

# Regeringens lagförslag

## 1 Förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Härigenom föreskrivs<sup>1</sup> följande.

### Syftet med lagen

1 § Syftet med denna lag är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för

1. samhällsviktiga tjänster inom sektorerna
  - energi,
  - transport,
  - bankverksamhet,
  - finansmarknadsinfrastruktur,
  - hälso- och sjukvård,
  - leverans och distribution av dricksvatten,
  - digital infrastruktur, och
2. digitala tjänster.

### Uttryck i lagen

2 § I lagen avses med

1. *nätverk och informationssystem*:
  - a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation,
  - b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller
  - c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna drifvas, användas, skyddas och underhållas,
2. *säkerhet i nätverk och informationssystem*: nätverks och informationssystemets förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem,
3. *samhällsviktig tjänst*: en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

<sup>1</sup> Jfr Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, i den ursprungliga lydelsen.

4. *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster, och som utgör en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst,

5. *internetbaserad marknadsplats*: en tjänst som gör det möjligt för konsumenter eller näringsidkare enligt definitionen i artikel 4.1 a respektive 4.1 b i Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning) att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare, antingen på webbplatsen för den internetbaserade marknadsplatsen eller på en webbplats som tillhör en näringsidkare och där datatjänster som tillhandahålls av en internetbaserad marknadsplats används,

6. *internetbaserad sökmotor*: en tjänst som gör det möjligt för användare att göra sökningar på i princip alla webbplatser eller webbplatser på ett visst språk genom en förfrågan om vilket ämne som helst i form av ett nyckelord, en fras eller någon annan inmatning, och som returnerar länkar som innehåller information om det begärda innehållet,

7. *molntjänst*: en tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser,

8. *NIS-direktivet*: Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen,

9. *företrädare*: en fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör och till vilken myndigheter kan vända sig, i stället för till leverantören, i frågor som gäller de skyldigheter som leverantören har enligt NIS-direktivet,

10. *incident*: en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem, och

11. *risk*: en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverk och informationssystem.

## Lagens tillämpningsområde

### 3 § Lagen gäller för

1. leverantörer av det slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst, under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (leverantörer av samhällsviktiga tjänster), och

2. juridiska personer som tillhandahåller en digital tjänst och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här (leverantörer av digitala tjänster).

I 10 § finns en bestämmelse som gäller för andra leverantörer.

**4 §** Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster och vad som avses med en betydande störning enligt 3 § första stycket 1.

## **Undantag från lagens tillämpningsområde**

### **Leverantörer av elektroniska kommunikationstjänster**

**5 §** Lagen gäller inte för företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och därför omfattas av kraven i 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation.

### **Leverantörer av betrodda tjänster**

**6 §** Lagen gäller inte för leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

### **Leverantörer av digitala tjänster som är mikroföretag eller små företag**

**7 §** Lagen gäller inte för leverantörer av digitala tjänster som är mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

### **Säkerhetskänslig verksamhet**

**8 §** Lagen gäller inte för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen (1996:627).

### **Leverantörer som omfattas av krav på informationssäkerhet i andra författningar**

**9 §** Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

### **Utseende av företrädare**

**10 §** En juridisk person som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom Europeiska unionen och inte heller har utsett en företrädare som är etablerad i en medlemsstat där tjänsterna erbjuds, ska, om inte något undantag från lagens tillämpningsområde enligt 5–9 §§ är tillämpligt, utse en sådan företrädare.

## Säkerhetsåtgärder

### Skyldigheter för leverantörer av samhällsviktiga tjänster

11 § Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

12 § Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 13 och 14 §§. I analysen ska det ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

13 § Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

14 § Leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

### Skyldigheter för leverantörer av digitala tjänster

15 § Leverantörer av digitala tjänster ska vidta de tekniska och organisatoriska åtgärder som de anser ändamålsenliga och proportionella och som hanterar risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller digitala tjänster inom Europeiska unionen. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

16 § Leverantörer av digitala tjänster ska vidta åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder. Skyldigheten gäller endast i förhållande till verkningar som sådana incidenter har på digitala tjänster som leverantören erbjuder inom Europeiska unionen. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

### Bemyndigande

17 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsåtgärder enligt 11–16 §§.

## **Incidentrapportering**

### **Rapporteringsskyldighet för leverantörer av samhällsviktiga tjänster**

**18 §** Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller. Rapporteringen ska göras till den myndighet som regeringen bestämmer.

### **Rapporteringsskyldighet för leverantörer av digitala tjänster**

**19 §** Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder inom Europeiska unionen. Rapporteringen ska göras till den myndighet som regeringen bestämmer.

### **Bemyndigande**

**20 §** Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapportering enligt 18 och 19 §§.

## **Tillsyn**

### **Tillsynsmyndighetens uppdrag**

**21 §** Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet. Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

**22 §** Tillsynsåtgärder när det gäller leverantörer av digitala tjänster får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att en leverantör inte uppfyller kraven i 15, 16 eller 19 §.

### **Anmälningsskyldighet för leverantörer av samhällsviktiga tjänster**

**23 §** Leverantörer av samhällsviktiga tjänster ska utan dröjsmål anmäla sig till tillsynsmyndigheten. Av en anmälan ska det framgå om leverantören tillhandahåller en samhällsviktig tjänst i två eller flera medlemsstater inom Europeiska unionen.

### **Tillsynsmyndighetens undersökningsbefogenheter**

**24 §** Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen.

**25 §** Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av lagen.

**26 §** Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 24 och 25 §§.

Ett sådant föreläggande får förenas med vite.

**27 §** Tillsynsmyndigheten får begära handräckning av Kronofogde-myndigheten för att genomföra de åtgärder som avses i 24 och 25 §§. Vid handräckning gäller bestämmelserna i utskökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

## **Ingripanden och sanktioner**

### **Åtgärdsförelägganden**

**28 §** Tillsynsmyndigheten får meddela de förelägganden som behövs för att leverantörer ska uppfylla kraven på utseende av företrädare, säkerhetsåtgärder och incidentrapportering enligt 10, 12–16, 18 och 19 §§ och enligt föreskrifter som har meddelats i anslutning till de paragraferna.

Ett sådant föreläggande får förenas med vite.

### **Sanktionsavgift**

**29 §** Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som underlåter att

1. göra en anmälan till tillsynsmyndigheten enligt 23 § eller enligt föreskrifter som har meddelats i anslutning till den paragrafen,
2. vidta säkerhetsåtgärder enligt någon av 12–16 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna, eller
3. rapportera incidenter enligt 18 eller 19 § eller enligt föreskrifter som har meddelats i anslutning till de paragraferna.

**30 §** En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

**31 §** När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om leverantören tidigare har begått en överträdelse och de kostnader som leverantören har undvikit till följd av överträdelsen.

**32 §** En sanktionsavgift får efterges helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

**33 §** En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

**34 §** En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

**35 §** En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

**36 §** En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

### **Föreskrifter om verkställighet**

**37 §** Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om verkställighet av denna lag.

### **Förordnande om att beslut ska gälla omedelbart**

**38 §** Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

### **Överklagande**

**39 §** Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

Denna lag träder i kraft den 1 augusti 2018.



## 2 Förslag till lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster

Härigenom föreskrivs att 8 § lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster ska ha följande lydelse.

*Lydelse enligt SFS 2018:000*                      *Föreslagen lydelse*

### 8 §

Lagen gäller inte för verksamhet som omfattas av *krav på säkerhetsskydd enligt säkerhetsskyddslagen (1996:627)*.

Lagen gäller inte för verksamhet som omfattas av säkerhetsskyddslagen (2018:000).

---

Denna lag träder i kraft den 1 april 2019.