EUROPAPARLAMENTET 2009 - 2014

Plenarhandling

A7-0103/2014

12.2.2014

***I
BETÄNKANDE

om förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Utskottet för den inre marknaden och konsumentskydd

Föredragande: Andreas Schwab

Rådgivande utskotts föredragande (*):
Pilar del Castillo Vera, utskottet för industrifrågor, forskning och energi
Carl Schlyter, utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

(*) Förfarande med associerade utskott – artikel 50 i arbetsordningen

Teckenförklaring

*	Samrådsförfarande
***	Godkännandeförfarande
***I	Ordinarie lagstiftningsförfarande (första behandlingen)
***II	Ordinarie lagstiftningsförfarande (andra behandlingen)
***III	Ordinarie lagstiftningsförfarande (tredje behandlingen)

(Det angivna förfarandet baseras på den rättsliga grund som angetts i förslaget till akt.)

Ändringsförslag till ett förslag till akt

När parlamentets ändringsförslag utformas i två spalter gäller följande:

Text som utgår markeras med ***fetkursiv stil*** i vänsterspalten. Text som ersätts markeras med ***fetkursiv stil*** i båda spalterna. Ny text markeras med ***fetkursiv stil*** i högerspalten.

De två första raderna i hänvisningen ovanför varje ändringsförslag anger vilket textavsnitt som avses i det förslag till akt som behandlas. Om ett ändringsförslag avser en befintlig akt som förslaget till akt är avsett att ändra innehåller hänvisningen även en tredje och en fjärde rad. Den tredje raden anger den befintliga akten och den fjärde vilken bestämmelse i denna akt som ändringsförslaget avser.

När parlamentets ändringsförslag utformas som en konsoliderad text gäller följande:

Nya textdelar markeras med ***fetkursiv stil***. Textdelar som utgår markeras med symbolen ▌ eller med genomstrykning. Textdelar som ersätts anges genom att ny text markeras med ***fetkursiv stil*** och text som utgår stryks eller markeras med genomstrykning.
Sådana ändringar som endast är tekniska och som gjorts av de berörda avdelningarna vid färdigställandet av den slutliga texten markeras däremot inte.

INNEHÅLL

Sida

(*) Förfarande med associerade utskott – artikel 50 i arbetsordningen

FÖRSLAG TILL EUROPAPARLAMENTETS LAGSTIFTNINGSRESOLUTION

om förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

(Ordinarie lagstiftningsförfarande: första behandlingen)

Europaparlamentet utfärdar denna resolution

– med beaktande av kommissionens förslag till Europaparlamentet och rådet (COM(2013)0048),

– med beaktande av artiklarna 294.2 och 114 i fördraget om Europeiska unionens funktionssätt, i enlighet med vilka kommissionen har lagt fram sitt förslag för parlamentet (C7-0035/2013),

– med beaktande av artikel 294.3 i fördraget om Europeiska unionens funktionssätt,

– med beaktande av artikel 55 i arbetsordningen,

– med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande av den 22 maj 2013[1],

– med beaktande av sin resolution av den 12 september 2013 om EU:s strategi för it-säkerhet: en öppen, säker och trygg cyberrymd[2],

– med beaktande av betänkandet från utskottet för den inre marknaden och konsumentskydd och yttrandena från utskottet för industrifrågor, forskning och energi, utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor och utskottet för utrikesfrågor (A7-0103/2014).

1. Europaparlamentet antar nedanstående ståndpunkt vid första behandlingen.

2. Europaparlamentet uppmanar kommissionen att lägga fram en ny text för parlamentet om den har för avsikt att väsentligt ändra sitt förslag eller ersätta det med ett nytt.

3. Europaparlamentet uppdrar åt talmannen att översända parlamentets ståndpunkt till rådet, kommissionen och de nationella parlamenten.

Ändringsförslag 1

Förslag till direktiv

[1] EUT C 0, 0.0.0000, s .0./Ännu ej offentliggjort i EUT.
[2] Antagna texter, P7_TA(2013)0376.

Skäl 1

Kommissionens förslag	*Ändringsförslag*
(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion.	(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning ***för EU-medborgarnas frihet och övergripande säkerhet samt*** för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion.

Ändringsförslag 2

Förslag till direktiv
Skäl 2

Kommissionens förslag	*Ändringsförslag*
(2) ***Avsiktliga eller oavsiktliga*** säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.	(2) Säkerhetsincidenter blir allt mer omfattande och ***vanliga och deras inverkan allt kraftigare***, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. ***Dessa system kan också bli ett lätt mål för avsiktligt sabotage som går ut på att skada dem eller avbryta driften.*** Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas ***och investerares*** förtroende och medföra allvarliga konsekvenser för unionens ekonomi ***samt i slutändan hota EU-medborgarnas välbefinnande och EU-medlemsstaternas förmåga att skydda sig själva och garantera säkerheten för kritiska infrastrukturer***.

Ändringsförslag 3

Förslag till direktiv
Skäl 3

Kommissionens förslag	*Ändringsförslag*
	(3a) Eftersom vanliga orsaker till systemfel fortsatt är oavsiktliga, exempelvis naturliga orsaker eller mänskliga misstag, bör infrastrukturen kunna stå emot både avsiktliga och oavsiktliga störningar, och operatörer som driver kritisk infrastruktur bör utforma motståndskraftsbaserade system.

Ändringsförslag 4

Förslag till direktiv
Skäl 4

Kommissionens förslag	*Ändringsförslag*
(4) En samarbetsmekanism bör inrättas på unionsnivå för att möjliggöra informationsutbyte och samordning av upptäckt och ***samordnade*** svarsåtgärder när det gäller nät- och informationssäkerhet. För att denna mekanism ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå av nät- och informationssäkerhet på det egna territoriet. Minimikrav avseende säkerhet bör också gälla för ***offentliga förvaltningar och operatörer*** av ***kritisk*** informationsinfrastrukturer, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras.	(4) En samarbetsmekanism bör inrättas på unionsnivå för att möjliggöra informationsutbyte och samordning av ***förebyggande åtgärder,*** upptäckt och svarsåtgärder när det gäller nät- och informationssäkerhet. För att denna mekanism ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå av nät- och informationssäkerhet på det egna territoriet. Minimikrav avseende säkerhet bör också gälla ***åtminstone*** för ***vissa marknadsoperatörer*** av informationsinfrastrukturer, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras. ***Börsnoterade företag bör uppmuntras att på frivillig basis offentliggöra incidenter i sina redovisningar. Den rättsliga ramen bör baseras på behovet av att skydda medborgarens privatliv och integritet. Nätverket för varningar om hot mot kritisk infrastruktur (Ciwin) bör utvidgas till de marknadsoperatörer som omfattas av detta direktiv.***

Ändringsförslag 5

Förslag till direktiv
Skäl 4a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4a) Offentliga förvaltningar bör på grund av sitt allmännyttiga uppdrag förvalta och skydda sina egna nätverk och informationssystem med vederbörlig aktsamhet, medan detta direktiv bör vara inriktat på kritisk infrastruktur som är nödvändig för att upprätthålla viktig ekonomisk och samhällelig verksamhet inom områdena energi, transport, bankverksamhet, finansmarknadsinfrastrukturer samt hälso- och sjukvård. Mjukvaruutvecklare och hårdvarutillverkare bör inte omfattas av detta direktiv.

Ändringsförslag 6

Förslag till direktiv
Skäl 4b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4b) Samarbete och samordning mellan de relevanta unionsmyndigheterna, vice ordföranden för kommissionen/den höga representanten – med ansvar för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken – och EU:s samordnare för kampen mot terrorism bör garanteras i fall där incidenter som har en betydande inverkan förefaller uppträda i form av yttre hot och terroristverksamhet.

Ändringsförslag 7

Förslag till direktiv
Skäl 6

Kommissionens förslag	*Ändringsförslag*
(6) Den befintliga kapaciteten räcker inte för att säkerställa en hög nivå av nät- och informationssäkerhet i unionen. Medlemsstaterna har väldigt olika nivåer av beredskap, vilket leder till fragmenterade angreppssätt i unionen. Resultatet blir olika grad av skydd för konsumenter och företag, vilket undergräver den allmänna nät- och informationssäkerhetsnivån i unionen. Avsaknaden av gemensamma minimikrav för ***offentliga förvaltningar och*** marknadsoperatörer gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå.	(6) Den befintliga kapaciteten räcker inte för att säkerställa en hög nivå av nät- och informationssäkerhet i unionen. Medlemsstaterna har väldigt olika nivåer av beredskap, vilket leder till fragmenterade angreppssätt i unionen. Resultatet blir olika grad av skydd för konsumenter och företag, vilket undergräver den allmänna nät- och informationssäkerhetsnivån i unionen. Avsaknaden av gemensamma minimikrav för marknadsoperatörer gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå. ***Universitet och forskningscentrum har en avgörande roll när det gäller att främja forskning, utveckling och innovation på dessa områden, och de bör ges adekvat finansiering.***

Ändringsförslag 8

Förslag till direktiv
Skäl 7

Kommissionens förslag	*Ändringsförslag*
(7) Effektiva reaktioner på utmaningarna på nät- och informationssäkerhetsområdet förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam lägsta nivå för kapacitetsuppbyggnad och planering, utbyte av information och samordning av åtgärder samt gemensamma minimikrav avseende säkerhet ***för alla berörda marknadsoperatörer och offentliga förvaltningar***.	(7) Effektiva reaktioner på utmaningarna på nät- och informationssäkerhetsområdet förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam lägsta nivå för kapacitetsuppbyggnad och planering***, utveckling av tillräcklig kompetens inom it-säkerhet***, utbyte av information och samordning av åtgärder samt gemensamma minimikrav avseende säkerhet. ***Gemensamma minimistandarder bör***

	tillämpas i enlighet med relevanta rekommendationer från samordningsgrupper för it-säkerhet (Cyber Security Coordination Groups – CSGC).

Ändringsförslag 9

Förslag till direktiv
Skäl 8

Kommissionens förslag	*Ändringsförslag*
(8) Bestämmelserna i detta direktiv bör inte påverka varje enskild medlemsstats möjligheter att vidta de åtgärder som är nödvändiga för att skydda sina väsentliga säkerhetsintressen, för att skydda allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och åtal av brott. Enligt artikel 346 i EUF-fördraget ska ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.	(8) Bestämmelserna i detta direktiv bör inte påverka varje enskild medlemsstats möjligheter att vidta de åtgärder som är nödvändiga för att skydda sina väsentliga säkerhetsintressen, för att skydda allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och åtal av brott. Enligt artikel 346 i EUF-fördraget ska ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. ***Ingen medlemsstat är skyldig att avslöja säkerhetsskyddsklassificerade EU-uppgifter enligt rådets beslut av den 31 mars 2011 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2011/292/EU), information som omfattas av sekretessavtal eller informella sekretessavtal, t.ex. Traffic Light Protocol.***

Motivering

Syftet med detta ändringsförslag är att klargöra hur sekretessbelagd information hanteras inom ramen för direktivet.

Ändringsförslag 10

Förslag till direktiv
Skäl 9

Kommissionens förslag	*Ändringsförslag*
(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå utarbeta planer för samarbete om nät- och informationssäkerhet ***med*** grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter.	(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå ***– på grundval av de minimikrav som anges i detta direktiv och med beaktande av vikten av att respektera och skydda privatlivet och personuppgifter –*** utarbeta planer för samarbete om nät- och informationssäkerhet ***vilka uppfyller*** grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter. ***Varje medlemsstat bör därför vara skyldig att uppfylla gemensamma standarder för uppgifters format och utbytbarheten av uppgifter som ska utbytas och utvärderas. Medlemsstaterna bör kunna be om stöd från Europeiska byrån för nät- och informationssäkerhet (Enisa) i utvecklingen av sina nationella strategier för nät- och informationssäkerhet, på grundval av en gemensam grundläggande strategisk plan för nät- och informationssäkerhet.***

Ändringsförslag 11

Förslag till direktiv
Skäl 10a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(10a) På grund av skillnaderna i nationella förvaltningsstrukturer och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsmyndigheter och undvika överlappning, bör medlemsstaterna kunna

utse mer än en nationell behörig myndighet som ansvarar för att utföra arbetsuppgifter som rör säkerheten i marknadsoperatörernas nät och informationssystem enligt detta direktiv. För att se till att samarbetet och kommunikationen över gränserna fungerar smidigt måste emellertid varje medlemsstat, utan att det påverkar sektorsspecifika regleringsarrangemang, utse endast en nationell gemensam kontaktpunkt som ansvarar för det gränsöverskridande samarbetet på unionsnivå. Om det är nödvändigt på grund av medlemsstatens konstitutionella struktur eller andra bestämmelser bör en medlemsstat kunna utse endast en myndighet som ska utföra den behöriga myndighetens och den gemensamma kontaktpunktens uppgifter. De behöriga myndigheterna och de gemensamma kontaktpunkterna bör vara civila organ som är föremål för fullständig demokratisk kontroll, och de bör inte utföra uppgifter på underrättelse-, brottsbekämpnings- eller försvarsrelaterade områden eller på något sätt vara organisatoriskt kopplade till organ som är verksamma på de områdena.

Ändringsförslag 12

Förslag till direktiv
Skäl 11

Kommissionens förslag	*Ändringsförslag*
(11) Samtliga medlemsstater bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, reagera på och begränsa effekterna av incidenter och risker vad gäller nät och informationssystem. Välfungerade incidenthanteringsorganisationer som uppfyller grundläggande krav bör därför inrättas i alla medlemsstater för att	(11) Samtliga medlemsstater ***och marknadsoperatörer*** bör ha både den tekniska och organisatoriska kapacitet som krävs för att ***när som helst*** förebygga, upptäcka, reagera på och begränsa effekterna av incidenter och risker vad gäller nät och informationssystem. ***Säkerhetssystem för offentlig förvaltning bör vara säkra och stå under demokratisk***

garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå.	***kontroll och granskning. Deras gängse nödvändiga utrustning och kapacitet bör följa gemensamt överenskomna tekniska standarder samt operativa standardförfaranden.*** Välfungerade incidenthanteringsorganisationer ***(Cert)*** som uppfyller grundläggande krav bör därför inrättas i alla medlemsstater för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. ***Dessa incidenthanteringsorganisationer bör kunna interagera på grundval av gemensamma tekniska standarder och operativa standardförfaranden. Eftersom de befintliga incidenthanteringsorganisationerna har olika karaktär och svarar mot olika behov och aktörer, bör medlemsstaterna garantera att åtminstone en incidenthanteringsorganisation tillhandahåller tjänster till var och en av de sektorer som avses i listan över marknadsoperatörer i detta direktiv. Medlemsstaterna bör säkerställa att incidenthanteringsorganisationerna har tillräckliga medel för att delta i gränsöverskridande samarbete i de befintliga internationella och unionsbaserade samarbetsnätverken.***

Motivering

Interoperabiliteten måste garanteras.

Ändringsförslag 13

Förslag till direktiv
Skäl 12

Kommissionens förslag	*Ändringsförslag*
(12) På grundval av de betydande framsteg som gjorts inom det europeiska forumet för medlemsstaterna (EFMS) när det gäller att främja diskussioner och utbyten av bästa	(12) På grundval av de betydande framsteg som gjorts inom det europeiska forumet för medlemsstaterna (EFMS) när det gäller att främja diskussioner och utbyten av bästa

praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid cyberkriser bör medlemsstaterna och kommissionen bilda ett nätverk som för samman dem för kontinuerlig kommunikation och stöder deras samarbete. En sådan säker och effektiv samarbetsmekanism bör skapa förutsättningar för ett strukturerat och samordnat genomförande av informationsutbyte, upptäckt och svarsåtgärder på unionsnivå.

praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid cyberkriser bör medlemsstaterna och kommissionen bilda ett nätverk som för samman dem för kontinuerlig kommunikation och stöder deras samarbete. En sådan säker och effektiv samarbetsmekanism***, om lämpligt inklusive marknadsoperatörers deltagande,*** bör skapa förutsättningar för ett strukturerat och samordnat genomförande av informationsutbyte, upptäckt och svarsåtgärder på unionsnivå.

Ändringsförslag 14

Förslag till direktiv
Skäl 13

Kommissionens förslag	*Ändringsförslag*
(13) ***Europeiska byrån för nät- och informationssäkerhet (***Enisa***)*** bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och främja utbyte av bästa praxis. Vid tillämpningen av detta direktiv bör kommissionen i synnerhet konsultera Enisa. För att medlemsstaterna och kommissionen i rätt tid ska få den information som behövs bör tidiga varningar om incidenter och risker lämnas inom samarbetsnätverket. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsnätverket också fungera som ett instrument för utbyte av bästa praxis och bistå sina medlemmar vid kapacitetsuppbyggnad samt leda organiserandet av sakkunnigbedömning och nät- och informationssäkerhetsövningar.	(13) Enisa bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och främja utbyte av bästa praxis. Vid tillämpningen av detta direktiv bör kommissionen ***och medlemsstaterna*** i synnerhet konsultera Enisa. För att medlemsstaterna och kommissionen i rätt tid ska få den information som behövs bör tidiga varningar om incidenter och risker lämnas inom samarbetsnätverket. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsnätverket också fungera som ett instrument för utbyte av bästa praxis och bistå sina medlemmar vid kapacitetsuppbyggnad samt leda organiserandet av sakkunnigbedömning och nät- och informationssäkerhetsövningar.

Ändringsförslag 15

Förslag till direktiv
Skäl 13a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(13a) Medlemsstaterna bör vid behov kunna använda eller anpassa befintliga organisationsstrukturer eller strategier vid tillämpningen av bestämmelserna i detta direktiv.

Ändringsförslag 16

Förslag till direktiv
Skäl 14

Kommissionens förslag	*Ändringsförslag*
(14) En säker infrastruktur bör upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas inom samarbetsnätverket. Utan att det påverkar medlemsstaternas skyldighet att anmäla incidenter och risker med en unionsdimension till samarbetsnätverket bör medlemsstater inte få tillgång till konfidentiell information från andra medlemsstater förrän de kan visa att deras tekniska och finansiella resurser, personalresurser och kommunikationsinfrastruktur garanterar att de kan delta i nätverket på ett effektivt, verkningsfullt och säkert sätt.	(14) En säker infrastruktur bör upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas inom samarbetsnätverket. ***Befintliga strukturer i unionen bör utnyttjas till fullo i detta syfte.*** Utan att det påverkar medlemsstaternas skyldighet att anmäla incidenter och risker med en unionsdimension till samarbetsnätverket bör medlemsstater inte få tillgång till konfidentiell information från andra medlemsstater förrän de kan visa att deras tekniska och finansiella resurser, personalresurser och kommunikationsinfrastruktur garanterar att de kan delta i nätverket på ett effektivt, verkningsfullt och säkert sätt***, med insynsvänliga metoder***.

Ändringsförslag 17

Förslag till direktiv
Skäl 15

Kommissionens förslag	*Ändringsförslag*
(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor.	(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor.

Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och utbyta information och bästa praxis ***i*** utbyte ***mot*** operativt stöd vid incidenter.	Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och ***sinsemellan*** utbyta information och bästa praxis***, inklusive ömsesidigt*** utbyte ***av relevant information,*** operativt stöd ***och strategiskt analyserad*** information vid incidenter. ***För att effektivt uppmuntra utbyte av information och bästa praxis är det mycket viktigt att se till att marknadsoperatörer som deltar i sådana utbyten inte missgynnas till följd av att de samarbetar. Tillräckliga skyddsmekanismer behövs för att inte sådant samarbete ska utsätta dessa operatörer för högre efterlevnadsrisk eller nya ansvarsskyldigheter enligt bland annat lagstiftningen om konkurrens, immateriella rättigheter, uppgiftsskydd eller it-brottslighet, och inte heller för ökade operativa risker eller säkerhetsrisker.***

Ändringsförslag 18

Förslag till direktiv
Skäl 16

Kommissionens förslag	*Ändringsförslag*
(16) För att säkra öppenhet och insyn och informera ***EU-medborgare*** och marknadsoperatörer ordentligt bör de ***behöriga myndigheterna*** skapa en gemensam webbplats för ***offentliggörande av*** sådan information om incidenter ***och*** risker som inte är konfidentiell.	(16) För att säkra öppenhet och insyn och informera ***unionsmedborgare*** och marknadsoperatörer ordentligt bör de ***gemensamma kontaktpunkterna*** skapa en gemensam ***unionsomfattande*** webbplats för ***att offentliggöra*** sådan information om incidenter***,*** risker ***och riskreduceringssätt*** som inte är konfidentiell ***och för att vid behov ge råd om lämpliga underhållsåtgärder***. ***Informationen på webbplatsen bör vara tillgänglig oberoende av vilken apparat som används. Offentliggörandet av personuppgifter på denna webbplats bör vara begränsat till vad som är nödvändigt,***

	och uppgifterna bör vara så anonymiserade som möjligt.

Ändringsförslag 19

Förslag till direktiv
Skäl 18

Kommissionens förslag	*Ändringsförslag*
(18) På grundval av i synnerhet de nationella erfarenheterna av krishantering bör kommissionen och medlemsstaterna, i samarbete med Enisa, utarbeta en unionsplan för nät- och informationssäkerhetssamarbete som omfattar samarbetsmekanismer för att bemöta risker och incidenter. Planen bör vederbörligen beaktas när tidiga varningar görs inom samarbetsnätverket.	(18) På grundval av i synnerhet de nationella erfarenheterna av krishantering bör kommissionen och medlemsstaterna, i samarbete med Enisa, utarbeta en unionsplan för nät- och informationssäkerhetssamarbete som omfattar samarbetsmekanismer***, bästa praxis och operationsmönster*** för att ***förebygga, upptäcka, rapportera och*** bemöta risker och incidenter. Planen bör vederbörligen beaktas när tidiga varningar görs inom samarbetsnätverket.

Ändringsförslag 20

Förslag till direktiv
Skäl 19

Kommissionens förslag	*Ändringsförslag*
(19) Anmälan av en tidig varning inom nätverket bör endast krävas när den berörda incidenten eller risken är av sådan omfattning och så allvarlig att den är eller kan bli så betydande att det är nödvändigt med information eller samordning av svarsåtgärderna på unionsnivå. Tidiga varningar bör därför begränsas till ***faktiska eller potentiella*** incidenter eller risker som är av snabbt ökande omfattning, som överstiger den nationella beredskapen eller som påverkar mer än en medlemsstat. För att möjliggöra en riktig utvärdering bör all information av relevans för bedömningen av risken eller incidenten meddelas	(19) Anmälan av en tidig varning inom nätverket bör endast krävas när den berörda incidenten eller risken är av sådan omfattning och så allvarlig att den är eller kan bli så betydande att det är nödvändigt med information eller samordning av svarsåtgärderna på unionsnivå. Tidiga varningar bör därför begränsas till incidenter eller risker som är av snabbt ökande omfattning, som överstiger den nationella beredskapen eller som påverkar mer än en medlemsstat. För att möjliggöra en riktig utvärdering bör all information av relevans för bedömningen av risken eller incidenten meddelas samarbetsnätverket.

samarbetsnätverket.

Ändringsförslag 21

Förslag till direktiv
Skäl 20

Kommissionens förslag	*Ändringsförslag*
(20) Vid mottagandet av en tidig varning, och vid sin bedömning av den, bör de ***behöriga myndigheterna*** enas om samordnade svarsåtgärder i enlighet med unionens plan för nät- och informationssäkerhetssamarbete. ***Behöriga myndigheter*** bör***, liksom kommissionen,*** informeras om de åtgärder som vidtas på nationell nivå till följd av de samordnade svarsåtgärderna.	(20) Vid mottagandet av en tidig varning, och vid sin bedömning av den, bör de ***gemensamma kontaktpunkterna*** enas om samordnade svarsåtgärder i enlighet med unionens plan för nät- och informationssäkerhetssamarbete. ***De gemensamma kontaktpunkterna, Enisa och kommissionen*** bör informeras om de åtgärder som vidtas på nationell nivå till följd av de samordnade svarsåtgärderna.

Ändringsförslag 22

Förslag till direktiv
Skäl 21

Kommissionens förslag	*Ändringsförslag*
(21) I och med att nät- och informationssäkerhetsproblemen är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyten och främja ett gemensamt sätt att hantera nät- och informationssäkerhetsfrågor.	(21) I och med att nät- och informationssäkerhetsproblemen är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyten och främja ett gemensamt sätt att hantera nät- och informationssäkerhetsfrågor. ***Varje ram för detta internationella samarbete bör omfattas av bestämmelserna i direktiv 95/46/EG och förordning (EG) nr 45/2001.***

Ändringsförslag 23

Förslag till direktiv
Skäl 22

Kommissionens förslag	*Ändringsförslag*
(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på ***offentliga förvaltningar och marknadsoperatörer***. En kultur av riskhantering***, som*** inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Lika konkurrensvillkor för alla krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.	(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på ***marknadsoperatörerna***. En kultur av riskhantering***, nära samarbete och förtroende vilken*** inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna ***och incidenterna, oavsett om det rör sig om avsiktliga eller oavsiktliga sådana***, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Lika konkurrensvillkor ***som gäller*** för alla ***på ett tillförlitligt sätt*** krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.

Ändringsförslag 24

Förslag till direktiv
Skäl 24

Kommissionens förslag	*Ändringsförslag*
(24) Dessa skyldigheter bör utvidgas bortom sektorn för elektronisk kommunikation till viktiga leverantörer av informationssamhällets tjänster, enligt definitionen i Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster[4], som ligger till grund för informationssamhällets tjänster i senare led eller onlineverksamhet, t.ex. e-handelsplattformar, ***internetbelningsslussar***, sociala nät, sökmotorer, molntjänster och onlineförsäljning av tillämpningar. ***Störningar i denna typ av informationssamhällestjänster hindrar tillhandahållandet av andra***	(24) Dessa skyldigheter bör utvidgas bortom sektorn för elektronisk kommunikation till ***att omfatta operatörer av infrastruktur vilka är starkt beroende av informations- och kommunikationsteknik och vilka behövs för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, finansmarknadsinfrastrukturer och hälso- och sjukvård. Störningar i dessa nät och informationssystem skulle påverka den inre marknaden. Även om skyldigheterna enligt detta direktiv inte bör utvidgas till att omfatta*** viktiga leverantörer av informationssamhällets tjänster, enligt definitionen i Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett

informationssamhällestjänster som är beroende av dem. Programutvecklare och hårdvarutillverkare är inte leverantörer av informationssamhällets tjänster och omfattas därför inte. Dessa skyldigheter bör också utvidgas till att omfatta offentliga förvaltningar och operatörer av kritisk infrastruktur som är starkt beroende av informations- och kommunikationsteknik och som behövs för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, börser och hälso- och sjukvård. Störningar i dessa nät och informationssystem skulle påverka den inre marknaden.

informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster[4], som ligger till grund för informationssamhällets tjänster i senare led eller onlineverksamhet, t.ex. e-handelsplattformar, ***internetbetalningsslussar***, sociala nät, sökmotorer, molntjänster ***i allmänhet*** och onlineförsäljning av tillämpningar***, kan dessa viktiga leverantörer av informationssamhällets tjänster, på frivillig basis och om lämpligt i det specifika fallet enligt deras bedömning, informera den behöriga myndigheten eller den gemensamma kontaktpunkten om incidenter i nätverkssäkerheten. Den behöriga myndigheten eller den gemensamma kontaktpunkten bör, om möjligt, till de marknadsoperatörer som informerat om incidenten lämna strategiskt analyserad information som bidrar till att avhjälpa säkerhetshotet.***

Ändringsförslag 25

Förslag till direktiv
Skäl 24a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(24a) Även om hårdvaru- och mjukvaruleverantörer inte är marknadsoperatörer på samma sätt som de som omfattas av detta direktiv, främjar deras produkter säkerheten för nät och informationssystem. De spelar därför en viktig roll när det gäller att göra det möjligt för marknadsoperatörer att säkra sina nät och informationsinfrastrukturer. Med tanke på att hårdvaru- och mjukvaruprodukter redan omfattas av befintliga regler om produktansvar bör medlemsstaterna se till att de reglerna tillämpas i vederbörlig ordning.

Ändringsförslag 26

Förslag till direktiv
Skäl 25

Kommissionens förslag	*Ändringsförslag*
(25) Tekniska och organisatoriska åtgärder som införs för ***offentliga förvaltningar och*** marknadsoperatörer bör inte omfatta krav på att en viss kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.	(25) Tekniska och organisatoriska åtgärder som införs för marknadsoperatörer bör inte omfatta krav på att en viss kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.

Ändringsförslag 27

Förslag till direktiv
Skäl 26

Kommissionens förslag	*Ändringsförslag*
(26) ***De offentliga förvaltningarna och*** marknadsoperatörerna bör garantera säkerheten för de nät och system som står under deras kontroll. Det rör sig framför allt om privata nät och system som antingen förvaltas av deras interna it-personal eller vars säkerhet har lagts ut på entreprenad. Säkerheten och anmälningsskyldigheterna bör gälla för relevanta marknadsoperatörer ***och offentliga förvaltningar*** oavsett om de själva sköter underhållet på sina nät och informationssystem internt eller om de lägger ut uppgifterna på entreprenad.	(26) Marknadsoperatörerna bör garantera säkerheten för de nät och system som står under deras kontroll. Det rör sig framför allt om privata nät och system som antingen förvaltas av deras interna it-personal eller vars säkerhet har lagts ut på entreprenad. Säkerheten och anmälningsskyldigheterna bör gälla för relevanta marknadsoperatörer oavsett om de själva sköter underhållet på sina nät och informationssystem internt eller om de lägger ut uppgifterna på entreprenad.

Ändringsförslag 28

Förslag till direktiv
Skäl 28

Kommissionens förslag	*Ändringsförslag*
(28) Behöriga myndigheter bör se till att upprätthålla informella och tillförlitliga	(28) Behöriga myndigheter ***och gemensamma kontaktpunkter*** bör se till

kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna bör allmänhetens intresse av att få information om hot vägas mot eventuella negativ inverkan på ryktet och affärerna för de ***offentliga förvaltningar och*** marknadsoperatörer som rapporterar incidenter. Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar ***släpps***.

att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. ***Behöriga myndigheter och gemensamma kontaktpunkter bör informera tillverkare och leverantörer av berörda IKT-produkter och IKT-tjänster om incidenter som har en betydande inverkan och som anmälts till dem.*** Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** bör allmänhetens intresse av att få information om hot vägas mot eventuella negativ inverkan på ryktet och affärerna för de marknadsoperatörer som rapporterar incidenter. Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter ***och gemensamma kontaktpunkter*** särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar ***satts i verket***. ***Den allmänna regeln bör vara att gemensamma kontaktpunkter inte bör lämna ut personuppgifter om dem som är inblandade i incidenter. Gemensamma kontaktpunkter bör lämna ut personuppgifter endast om det är nödvändigt och proportionellt för ändamålet.***

Ändringsförslag 29

Förslag till direktiv
Skäl 29

Kommissionens förslag	*Ändringsförslag*
(29) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att få fram tillräckligt med information från marknadsoperatörer ***och offentliga förvaltningar*** för att bedöma säkerhetsnivån för nät och	(29) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att få fram tillräckligt med information från marknadsoperatörer för att bedöma säkerhetsnivån för nät och informationssystem ***och mäta incidenters***

informationssystem liksom tillförlitliga och heltäckande data om faktiska incidenter som har inverkat på nätens och informationssystemens drift.	***antal, storlek och omfattning,*** liksom tillförlitliga och heltäckande data om faktiska incidenter som har inverkat på nätens och informationssystemens drift.

Ändringsförslag 30

Förslag till direktiv
Skäl 30

Kommissionens förslag	*Ändringsförslag*
(30) I många fall är det kriminell verksamhet som ligger bakom en incident. Incidenternas kriminella art kan misstänkas även om det inte finns några entydiga bevis från början. I sådana fall bör ett lämpligt samarbete mellan behöriga myndigheter och brottsbekämpande myndigheter ingå i effektiva och omfattande svarsåtgärder på hotet från säkerhetsincidenter. För att främja en säker, trygg och mer motståndskraftig miljö krävs i synnerhet en systematisk rapportering av incidenter som misstänks vara av kriminell art till de brottsbekämpande myndigheterna. Incidenters allvarliga kriminella art bör bedömas i ljuset av EU-lagstiftningen om it-brott.	(30) I många fall är det kriminell verksamhet som ligger bakom en incident. Incidenternas kriminella art kan misstänkas även om det inte finns några entydiga bevis från början. I sådana fall bör ett lämpligt samarbete mellan behöriga myndigheter***, gemensamma kontaktpunkter*** och brottsbekämpande myndigheter ***samt samarbete med Europols it-brottscentrum (EC3) och Enisa*** ingå i effektiva och omfattande svarsåtgärder på hotet från säkerhetsincidenter. För att främja en säker, trygg och mer motståndskraftig miljö krävs i synnerhet en systematisk rapportering av incidenter som misstänks vara av kriminell art till de brottsbekämpande myndigheterna. Incidenters allvarliga kriminella art bör bedömas i ljuset av EU-lagstiftningen om it-brott.

Ändringsförslag 31

Förslag till direktiv
Skäl 31

Kommissionens förslag	*Ändringsförslag*
(31) Säkerheten för personuppgifter äventyras ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna och dataskyddsmyndigheterna samarbeta och utbyta information ***om alla relevanta***	(31) Säkerheten för personuppgifter äventyras ofta till följd av incidenter. ***Medlemsstater och marknadsoperatörer bör skydda personuppgifter som lagras, behandlas eller överförs mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust***

frågor för att hantera personuppgiftsbrott till följd av incidenter. ***Medlemsstaterna ska genomföra*** skyldigheten att anmäla säkerhetsincidenter på ett sätt som minimerar den administrativa bördan om säkerhetsincidenten också är ett personuppgiftsbrott ***i linje med förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter***. ***Genom samarbete med de behöriga myndigheterna och dataskyddsmyndigheterna skulle*** Enisa ***kunna*** vara till hjälp genom att utveckla mekanismer ***och modeller*** för informationsutbyte ***så att det inte behövs två anmälningsmallar. Denna enda*** anmälningsmall skulle underlätta rapporteringen av incidenter som hotar säkerheten för personuppgifter och därigenom lätta den administrativa bördan för företag och offentliga förvaltningar.

eller ändring, och otillåten eller olaglig lagring, åtkomst, utlämning eller spridning, och garantera genomförandet av en säkerhetsstrategi för behandling av personuppgifter. I detta sammanhang bör de behöriga myndigheterna***, de gemensamma kontaktpunkterna*** och dataskyddsmyndigheterna samarbeta och utbyta information***, vid behov även med marknadsoperatörer,*** för att ***i enlighet med tillämpliga dataskyddsregler*** hantera personuppgiftsbrott till följd av incidenter. Skyldigheten att anmäla säkerhetsincidenter ***bör fullgöras*** på ett sätt som minimerar den administrativa bördan om säkerhetsincidenten också är ett personuppgiftsbrott ***som ska anmälas i enlighet med unionens dataskyddslagstiftning***. Enisa ***bör*** vara till hjälp genom att utveckla mekanismer för informationsutbyte ***och en gemensam*** anmälningsmall***, vilket*** skulle underlätta rapporteringen av incidenter som hotar säkerheten för personuppgifter och därigenom lätta den administrativa bördan för företag och offentliga förvaltningar.

Ändringsförslag 32

Förslag till direktiv
Skäl 32

Kommissionens förslag	*Ändringsförslag*
(32) Standardisering av säkerhetskrav är en marknadsdriven process. För att säkerställa en konvergerad tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade standarder för att garantera en hög säkerhetsnivå på unionsnivå. Därför kan ***det*** vara nödvändigt att ***utarbeta*** harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets	(32) Standardisering av säkerhetskrav är en marknadsdriven process ***av frivillig karaktär som bör möjliggöra för marknadsoperatörer att använda alternativa metoder för att uppnå åtminstone liknande resultat***. För att säkerställa en konvergerad tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade ***interoperabla*** standarder för att garantera en hög säkerhetsnivå på unionsnivå. Därför ***behöver tillämpning av öppna internationella standarder för nät-***

direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG[6].

och informationssäkerhet eller utformning av sådana verktyg övervägas. Ett ytterligare framsteg som kan vara nödvändigt ***är*** att ***det utarbetas*** harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG[6]. ***Särskilt bör Etsi, CEN och Cenelec uppdras att föreslå effektiva och ändamålsenliga öppna säkerhetsstandarder för unionen, där tekniska preferenser undviks så långt möjligt, och som bör vara lätthanterliga för små och medelstora marknadsoperatörer. Internationella standarder för it-säkerhet bör granskas noggrant för att säkerställa att de inte har kompromitterats och att de ger en tillräcklig säkerhetsnivå, och sålunda garanterar att den föreskrivna efterlevnaden av it-säkerhetsstandarder ökar unionens it-säkerhet som helhet och inte minskar den.***

[6] EUT L 316, 14.11.2012, s. 12.

[6] EUT L 316, 14.11.2012, s. 12.

Ändringsförslag 33

Förslag till direktiv
Skäl 33

Kommissionens förslag	*Ändringsförslag*
(33) Detta direktiv bör ses över ***med jämna mellanrum***, främst i syfte att avgöra behovet av modifieringar med hänsyn till	(33) Detta direktiv bör ***med jämna mellanrum*** ses över ***av kommissionen***, ***i samråd med alla berörda aktörer,*** främst i

den tekniska utvecklingen eller ändrade marknadsvillkor.	syfte att avgöra behovet av modifieringar med hänsyn till ***samhällsutvecklingen,*** den ***politiska utvecklingen, den*** tekniska utvecklingen eller ändrade marknadsvillkor.

Ändringsförslag 34

Förslag till direktiv
Skäl 34

Kommissionens förslag	*Ändringsförslag*
(34) För att se till att samarbetsnätverket fungerar på ett korrekt sätt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på ***fastställandet av de kriterier som en medlemsstat ska uppfylla för att ha rätt att delta*** i ***det*** säkra ***informationsutbytessystemet,*** ytterligare specificering av de händelser som utlöser tidig varning ***och definitionen av de omständigheter då marknadsoperatörer och offentliga förvaltningar är skyldiga att anmäla incidenter***.	(34) För att se till att samarbetsnätverket fungerar på ett korrekt sätt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på ***gemensamma standarder för samtrafik och säkerhet*** i ***den*** säkra ***informationsutbytesinfrastrukturen och*** ytterligare specificering av de händelser som utlöser tidig varning.

Ändringsförslag 35

Förslag till direktiv
Skäl 36

Kommissionens förslag	*Ändringsförslag*
(36) För att säkerställa enhetliga villkor för genomförandet av direktivet bör kommissionen ges genomförandebefogenheter när det gäller samarbetet mellan ***behöriga myndigheter*** och kommissionen inom samarbetsnätverket, ***tillträdet till den säkra infrastrukturen för informationsutbyte,*** unionens samarbetsplan för nät- och informationssäkerhet***,*** formaten och förfarandena för att ***informera***	(36) För att säkerställa enhetliga villkor för genomförandet av direktivet bör kommissionen ges genomförandebefogenheter när det gäller samarbetet mellan ***gemensamma kontaktpunkter*** och kommissionen inom samarbetsnätverket***, dock utan att det påverkar befintliga nationella samarbetsmekanismer***, unionens samarbetsplan för nät- och informationssäkerhet samt formaten och

allmänheten om incidenter ***samt standarderna och/eller de tekniska specifikationerna av betydelse för nät- och informationssäkerhet***. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter.

förfarandena för att ***rapportera*** om incidenter ***som har en betydande inverkan***. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter.

Motivering

Detta ändringsförslag ersätter ändringsförslag 20. Ändringsförslaget syftar till att korrigera ett fel i kommissionens förslag när det gäller innehållet i den planerade genomförandeakten och återspeglar det nya ändringsförslaget till artikel 9.3.

Ändringsförslag 36

Förslag till direktiv
Skäl 37

Kommissionens förslag	*Ändringsförslag*
(37) Vid tillämpningen av direktivet bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på EU-nivå, i synnerhet ***inom energi-***, ***transport- och*** hälso- och ***sjukvårdsområdet***.	(37) Vid tillämpningen av direktivet bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på EU-nivå, i synnerhet ***på områdena e-förvaltning, energi***, ***transport,*** hälso- och ***sjukvård och försvar***.

Ändringsförslag 37

Förslag till direktiv
Skäl 38

Kommissionens förslag	*Ändringsförslag*
(38) Information som ***den nationella regleringsmyndigheten*** anser vara konfidentiell i enlighet med unionslagstiftning och nationell lagstiftning om affärshemligheter, får ***endast*** utbytas med kommissionen ***och*** andra behöriga myndigheter när sådant utbyte är absolut	(38) Information som ***en behörig myndighet eller en gemensam kontaktpunkt*** anser vara konfidentiell i enlighet med unionslagstiftning och nationell lagstiftning om affärshemligheter, får utbytas med kommissionen***,*** ***kommissionens relevanta organ,***

nödvändigt för att tillämpa bestämmelserna i detta direktiv. Den information som utbyts bör begränsas till vad som är relevant och proportionellt för ändamålet med utbytet.

gemensamma kontaktpunkter och/eller andra behöriga ***nationella*** myndigheter ***endast*** när sådant utbyte är absolut nödvändigt för att tillämpa bestämmelserna i detta direktiv. Den information som utbyts bör begränsas till vad som är relevant***, nödvändigt*** och proportionellt för ändamålet med utbytet***, och den bör respektera på förhand fastställda kriterier för konfidentialitet och säkerhet – i enlighet med rådets beslut av den 31 mars 2011 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2011/292/EU) –, för information som omfattas av sekretessavtal och för informella sekretessavtal, t.ex. Traffic Light Protocol***.

Ändringsförslag 38

Förslag till direktiv
Skäl 39

Kommissionens förslag	*Ändringsförslag*
(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse och är därmed berättigad enligt artikel 7 i direktiv 95/46/EG. I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och	(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna ***eller gemensamma kontaktpunkterna*** kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse och är därmed berättigad enligt artikel 7 i direktiv 95/46/EG. I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till

kommissionens handlingar gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

Europaparlamentets, rådets och kommissionens handlingar gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

Ändringsförslag 39

Förslag till direktiv
Skäl 41a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(41a) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument har medlemsstaterna åtagit sig att i motiverade fall låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i ett direktiv och motsvarande delar i nationella instrument för införlivande. När det gäller detta direktiv anser lagstiftaren det vara motiverat att sådana dokument översänds.

Ändringsförslag 40

Förslag till direktiv
Artikel 1 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska	(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska

säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad ***och*** effektiv hantering och samordnade ***och*** effektiva svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.	säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad***,*** effektiv ***och ändamålsenlig*** hantering och samordnade***,*** effektiva ***och ändamålsenliga*** svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem***, med deltagande av relevanta aktörer***.

Ändringsförslag 41

Förslag till direktiv
Artikel 1 – punkt 2 – led c

Kommissionens förslag	*Ändringsförslag*
(c) Det fastställer säkerhetskrav för ***marknadsaktörer och offentliga förvaltningar***.	(c) Det fastställer säkerhetskrav för ***marknadsoperatörer***.

Ändringsförslag 42

Förslag till direktiv
Artikel 1 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. Detta direktiv påverkar inte heller tillämpningen av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och Europaparlamentets och rådets förordning om skydd för enskilda ***personer med avseende på behandling av*** personuppgifter och om ***det*** fria ***flödet av*** sådana uppgifter.	5. Detta direktiv påverkar inte heller tillämpningen av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och Europaparlamentets och rådets förordning ***(EG) nr 45/2001 av den 18 december 2000*** om skydd för enskilda ***då gemenskapsinstitutionerna och gemenskapsorganen behandlar*** personuppgifter och om ***den*** fria ***rörligheten för*** sådana uppgifter. ***Användningen av personuppgifter ska***

begränsas till vad som är absolut nödvändigt för syftena med detta direktiv, och uppgifterna ska vara så anonyma som möjligt, om inte fullständigt anonyma.

Ändringsförslag 43

Förslag till direktiv
Artikel 1a (ny)

Kommissionens förslag	*Ändringsförslag*
	Artikel 1a
	Skydd och behandling av personuppgifter
	1. All behandling av personuppgifter i medlemsstaterna med tillämpning av detta direktiv ska ske i enlighet med direktiven 95/46/EG och 2002/58/EG.
	2. All behandling av personuppgifter som utförs av kommissionen och Enisa med tillämpning av detta direktiv ska ske i enlighet med förordning (EG) nr 45/2001.
	3. All behandling av personuppgifter som utförs av Europeiska it-brottscentrumet inom Europol med tillämpning av detta direktiv ska ske i enlighet med beslut 2009/371/RIF.
	4. Behandlingen av personuppgifter ska vara rättvis och laglig och ska strikt begränsas till de minimiuppgifter som krävs för det syfte för vilket de behandlas. Personuppgifterna ska lagras på ett sätt som förhindrar identifiering av de registrerade under en längre tid än vad som är nödvändigt för det ändamål för vilket personuppgifterna behandlas.
	5. De anmälningar av incidenter som avses i artikel 14 ska inte påverka tillämpningen av de bestämmelser och skyldigheter i fråga om att anmäla personuppgiftsbrott som fastställs i artikel 4 i direktiv 2002/58/EG och i förordning (EU) nr 611/2013.

Ändringsförslag 44

Förslag till direktiv
Artikel 3 – led 1 – led b

Kommissionens förslag	*Ändringsförslag*
(b) apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av ***datorbehandlade*** uppgifter, samt	(b) apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av ***digitala*** uppgifter, samt

Ändringsförslag 45

Förslag till direktiv
Artikel 3 – led 1 – led c

Kommissionens förslag	*Ändringsförslag*
(c) ***datorbehandlade*** uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av element som omfattas av led a och b för att de skall kunna drivas, användas, skyddas och underhållas.	(c) ***digitala*** uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av element som omfattas av led a och b för att de skall kunna drivas, användas, skyddas och underhållas.

Ändringsförslag 46

Förslag till direktiv
Artikel 3 – led 2

Kommissionens förslag	*Ändringsförslag*
(2) säkerhet: förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem.	(2) säkerhet: förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem***;***

	”säkerhet” inkluderar passande tekniska apparater, lösningar och driftsförfaranden som garanterar att de säkerhetskrav som anges i detta direktiv är uppfyllda.

Ändringsförslag 47

Förslag till direktiv
Artikel 3 – led 3

Kommissionens förslag	*Ändringsförslag*
(3) risk: en omständighet eller händelse som har en potentiell negativ inverkan på säkerheten.	(3) risk: en ***rimligen identifierbar*** omständighet eller händelse som har en potentiell negativ inverkan på säkerheten.

Ändringsförslag 48

Förslag till direktiv
Artikel 3 – led 4

Kommissionens förslag	*Ändringsförslag*
(4) incident: en ***omständighet eller*** händelse som har en faktisk negativ inverkan på säkerheten.	(4) incident: en händelse som har en faktisk negativ inverkan på säkerheten.

Ändringsförslag 49

Förslag till direktiv
Artikel 3 – led 5

Kommissionens förslag	*Ändringsförslag*
(5) informationssamhällestjänst: tjänst enligt artikel 1.2 i direktiv 98/34/EG.	***utgår***

Ändringsförslag 50

Förslag till direktiv
Artikel 3 – led 7

Kommissionens förslag	*Ändringsförslag*
(7) incidenthantering: alla förfaranden som ***stödjer*** analys och begränsning av effekterna av en incident samt svarsåtgärder.	(7) incidenthantering: alla förfaranden som ***stöder upptäckt, förebyggande,*** analys och begränsning av effekterna av en incident samt svarsåtgärder.

Ändringsförslag 51

Förslag till direktiv
Artikel 3 – led 8 – led a

Kommissionens förslag	*Ändringsförslag*
(a) Leverantör av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster; en ej uttömmande förteckning över sådana tjänster finns i bilaga II.	***utgår***

Ändringsförslag 52

Förslag till direktiv
Artikel 3 – led 8 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena ***energi-***, ***transport-***, ***bank-***, ***börs-*** samt hälso- och ***sjukvårdsverksamhet***; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II.	(b) Operatör av infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena ***energi***, ***transport***, ***bankverksamhet***, ***finansmarknadsinfrastrukturer***, ***internetknutpunkter, försörjningskedjan för livsmedel*** samt hälso- och ***sjukvård, och då störningar eller förstörelse som gör att dessa funktioner inte kan upprätthållas skulle ha en betydande inverkan i en medlemsstat***; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II***, i den mån det berörda nätet och de berörda informationssystemen har en anknytning***

till verksamheternas kärntjänster.

Ändringsförslag 53

Förslag till direktiv
Artikel 3 – led 8a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(8a) incident som har en betydande inverkan: en incident som påverkar säkerheten och kontinuiteten för ett informationsnät eller informationssystem och som leder till betydande störning av centrala ekonomiska eller samhälleliga funktioner.

Ändringsförslag 54

Förslag till direktiv
Artikel 3 – led 11a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11a) reglerad marknad: reglerad marknad enligt definitionen i artikel 4.14 i Europaparlamentets och rådets direktiv 2004/39/EG[1a].
	[1a] Europaparlamentets och rådets direktiv 2004/39/EG av den 21 april 2004 om marknader för finansiella instrument (EUT L 45, 16.2.2005, s. 18).

Motivering

Genom ändringsförlaget anpassas definitionen till den förordning som väntas bli antagen av Europaparlamentet och rådet om marknader för finansiella instrument och om ändring av förordning [EMIR] om OTC-derivat, centrala motparter och transaktionsregister.

Ändringsförslag 55

Förslag till direktiv
Artikel 3 – led 11b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11b) multilateral handelsplattform (MTF-plattform): multilateral handelsplattform enligt definitionen i artikel 4.15 i direktiv 2004/39/EG.

Motivering

Genom ändringsförlaget anpassas definitionen till den förordning som väntas bli antagen av Europaparlamentet och rådet om marknader för finansiella instrument och om ändring av förordning [EMIR] om OTC-derivat, centrala motparter och transaktionsregister.

Ändringsförslag 56

Förslag till direktiv
Artikel 3 – led 11c (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11c) organiserad handelsplattform: ett multilateralt system eller en multilateral facilitet – dock inte en reglerad marknad, en multilateral handelsplattform eller en central motpart – som drivs av ett värdepappersföretag eller en marknadsoperatör och där flera tredje parters köp- och säljintressen i obligationer, strukturerade finansiella produkter, utsläppsrätter eller derivat kan interagera inom systemet så att detta leder till ett avtal i enlighet med avdelning II i direktiv 2004/39/EG.

Motivering

Genom ändringsförlaget infogas definitionen i linje med och beroende av hur det går med den förordning som väntas bli antagen av Europaparlamentet och rådet om marknader för finansiella instrument och om ändring av förordning [EMIR] om OTC-derivat, centrala motparter och transaktionsregister.

Ändringsförslag 57

Förslag till direktiv
Artikel 5 – punkt 1 – led ea (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ea) Medlemsstaterna kan begära hjälp av Enisa när det gäller att utveckla de nationella strategierna och nationella samarbetsplanerna för nät- och informationssäkerhet, på grundval av en gemensam grundläggande strategi i fråga om nät- och informationssäkerhet.

Ändringsförslag 58

Förslag till direktiv
Artikel 5 – punkt 2 – led a

Kommissionens förslag	*Ändringsförslag*
(a) En ***riskbedömningsplan*** för kartläggning av risker ***och*** bedömning av verkningarna av potentiella incidenter.	(a) En ***riskhanteringsram*** för ***att utveckla en metod för*** kartläggning***, rangordning, utvärdering och åtgärdande*** av risker***,*** bedömning av verkningarna av potentiella incidenter***, handlingsalternativ för förebyggande och kontroll samt för att fastställa kriterier för valet av möjliga motåtgärder***.

Motivering

Detta ändringsförslag ersätter ändringsförslag 29. Kommissionens förslag skulle ha varit alltför långtgående när det gäller frågor som rör medlemsstaternas nationella säkerhet och skulle ha gjort samarbetsplanen ogenomförbar och alltför komplex för att vara effektiv.

Ändringsförslag 59

Förslag till direktiv
Artikel 5 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Definition av roller och ansvarsområden för olika aktörer som deltar i genomförandet av ***planen***.	(b) Definition av roller och ansvarsområden för olika ***myndigheter och övriga*** aktörer som deltar i genomförandet av ***ramen***.

Ändringsförslag 60

Förslag till direktiv
Artikel 5 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Den nationella NIS-strategin och den nationella NIS-samarbetsplanen ska meddelas kommissionen inom ***en månad*** från antagandet.	3. Den nationella NIS-strategin och den nationella NIS-samarbetsplanen ska meddelas kommissionen inom ***tre månader*** från antagandet.

Ändringsförslag 61

Förslag till direktiv
Artikel 6 – rubriken

Kommissionens förslag	*Ändringsförslag*
Nationell behörig myndighet för säkerheten i nät och informationssystem	***Nationella behöriga myndigheter och gemensamma kontaktpunkter*** för säkerheten i nät och informationssystem

Ändringsförslag 62

Förslag till direktiv
Artikel 6 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska utse en ***behörig nationell myndighet*** för säkerheten i nät och informationssystem (den behöriga ***myndigheten***).	1. Varje medlemsstat ska utse en ***eller flera civila behöriga nationella myndigheter*** för säkerheten i nät och informationssystem (den ***eller de*** behöriga ***myndigheterna***).

Motivering

Detta ändringsförslag ersätter ändringsförslag 32 och syftar till att ytterligare specificera vilken typ av institution som bör utgöra behörig nationell myndighet.

Ändringsförslag 63

Förslag till direktiv
Artikel 6 – punkt 2a (ny)

Kommissionens förslag	*Ändringsförslag*
	2a. Om en medlemsstat utser mer än en behörig myndighet ska den utse en civil nationell myndighet, t.ex. en behörig myndighet, som nationell gemensam kontaktpunkt för säkerheten i nät och informationssystem (nedan kallad gemensam kontaktpunkt). Om en medlemsstat utser bara en behörig myndighet ska denna behöriga myndighet också vara den gemensamma kontaktpunkten.

Motivering

Detta ändringsförslag ersätter ändringsförslag 33 och ligger i linje med föredragandens nya ändringsförslag till artikel 6.1. Det syftar till att ytterligare specificera vilken typ av institution som bör fungera som gemensam kontaktpunkt.

Ändringsförslag 64

Förslag till direktiv
Artikel 6 – punkt 2b (ny)

Kommissionens förslag	*Ändringsförslag*
	2b. De behöriga myndigheterna och den gemensamma kontaktpunkten i en medlemsstat ska ha ett nära samarbete när det gäller skyldigheterna enligt detta direktiv.

Ändringsförslag 65

Förslag till direktiv
Artikel 6 – punkt 2c (ny)

Kommissionens förslag	*Ändringsförslag*
	2c. Den gemensamma kontaktpunkten ska se till att det finns ett gränsöverskridande samarbete med andra gemensamma kontaktpunkter.

Ändringsförslag 66

Förslag till direktiv
Artikel 6 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Medlemsstaterna ska se till att de behöriga myndigheterna har tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå detta direktivs syften. Medlemsstaterna ska se till att de ***behöriga myndigheterna*** samarbetar på ett effektivt och säkert sätt via det nätverk som avses i artikel 8.	3. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå detta direktivs syften. Medlemsstaterna ska se till att de ***gemensamma kontaktpunkterna*** samarbetar på ett ***ändamålsenligt,*** effektivt och säkert sätt via det nätverk som avses i artikel 8.

Ändringsförslag 67

Förslag till direktiv
Artikel 6 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. Medlemsstaterna ska se till att de behöriga myndigheterna får de anmälningar av incidenter som görs av ***offentliga förvaltningar och*** marknadsoperatörer såsom anges i artikel 14.2 och att de tilldelas de genomförande- och verkställighetsbefogenheter som avses i artikel 15.	4. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna, i tillämpliga fall i enlighet med punkt 2a i denna artikel,*** får de anmälningar av incidenter som görs av marknadsoperatörer såsom anges i artikel 14.2 och att de tilldelas de genomförande- och verkställighetsbefogenheter som avses i artikel 15.

Motivering

Detta ändringsförslag ersätter ändringsförslag 37. Det syftar till att klargöra de olika myndigheternas roll för att undvika dubbla anmälningar, både till de behöriga myndigheterna och till de gemensamma kontaktpunkterna. Med tanke på att incidenter inom vissa sektorer redan anmäls till unionsorgan bör dubbla anmälningar undvikas.

Ändringsförslag 68

Förslag till direktiv
Artikel 6 – punkt 4a (ny)

Kommissionens förslag	*Ändringsförslag*
	4a. Om det i unionslagstiftningen föreskrivs ett sektorsspecifikt tillsyns- eller regleringsorgan på unionsnivå, bland annat för säkerheten i nät och informationssystem, ska detta organ ta emot anmälningarna av incidenter i enlighet med artikel 14.2 från berörda marknadsoperatörer i sektorn och tilldelas de befogenheter för genomförande och efterlevnad som avses i artikel 15. Unionsorganet ska ha ett nära samarbete med de behöriga myndigheterna och den gemensamma kontaktpunkten i värdmedlemsstaten när det gäller dessa skyldigheter. Den gemensamma kontaktpunkten i värdmedlemsstaten ska företräda unionsorganet när det gäller de skyldigheter som fastställs i kapitel III.

Ändringsförslag 69

Förslag till direktiv
Artikel 6 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. De behöriga myndigheterna ska när så är lämpligt samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.	5. De behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ska när så är lämpligt samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.

Ändringsförslag 70

Förslag till direktiv
Artikel 6 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. Varje medlemsstat ska utan dröjsmål meddela kommissionen den ***behöriga myndighet*** som utses, denna myndighets uppgifter och alla senare ändringar av detta. Varje medlemsstat ska offentliggöra utnämningen av ***den*** behöriga ***myndigheten***.	6. Varje medlemsstat ska utan dröjsmål meddela kommissionen ***de behöriga myndigheter och*** den ***gemensamma kontaktpunkt*** som utses, denna myndighets uppgifter och alla senare ändringar av detta. Varje medlemsstat ska offentliggöra utnämningen av ***de*** behöriga ***myndigheterna***.

Ändringsförslag 71

Förslag till direktiv
Artikel 7 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska inrätta en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) ***som ansvarar*** för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.	1. Varje medlemsstat ska inrätta ***minst*** en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) ***för var och en av de sektorer*** som ***anges i bilaga II, med ansvar*** för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.

Ändringsförslag 72

Förslag till direktiv
Artikel 7 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. ***Incidenthanteringsorganisationen*** ska bedriva sin verksamhet under tillsyn av den behöriga myndigheten, som regelbundet ska bedöma om resurserna är tillräckliga, om ***mandatet är ändamålsenligt*** och om incidenthanteringsförfarandet är effektivt.	5. ***Incidenthanteringsorganisationerna*** ska bedriva sin verksamhet under tillsyn av den behöriga myndigheten ***eller den gemensamma kontaktpunkten***, som regelbundet ska bedöma om resurserna är tillräckliga, om ***mandaten är ändamålsenliga*** och om incidenthanteringsförfarandet är effektivt.

Ändringsförslag 73

Förslag till direktiv
Artikel 7 – punkt 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	5a. Medlemsstaterna ska se till att incidenthanteringsorganisationerna har tillräckliga personalresurser och ekonomiska resurser för att aktivt delta i internationella samarbetsnätverk, särskilt sådana nätverk på EU-nivå.

Ändringsförslag 74

Förslag till direktiv
Artikel 7 – punkt 5b (ny)

Kommissionens förslag	*Ändringsförslag*
	5b. Incidenthanteringsorganisationerna ska ges möjlighet och uppmuntras att inleda och delta i gemensamma övningar med andra incidenthanteringsorganisationer, med alla incidenthanteringsorganisationer i medlemsstaterna och med lämpliga institutioner i icke-medlemsstater samt med incidenthanteringsorganisationer inom multinationella och internationella institutioner såsom Nato och FN.

Ändringsförslag 75

Förslag till direktiv
Artikel 7 – punkt 5c (ny)

Kommissionens förslag	*Ändringsförslag*
	5c. Medlemsstaterna får be om stöd från Enisa eller från andra medlemsstater i utvecklingen av sina nationella incidenthanteringsorganisationer.

Ändringsförslag 76

Förslag till direktiv
Artikel 8 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. De ***behöriga myndigheterna och*** kommissionen ska bilda ett nätverk (samarbetsnätverk) för att samarbeta om risker och incidenter som påverkar nät och informationssystem.	1. De ***gemensamma kontaktpunkterna,*** kommissionen ***och Enisa*** ska bilda ett nätverk (***nedan kallat*** samarbetsnätverk) för att samarbeta om risker och incidenter som påverkar nät och informationssystem.

Ändringsförslag 77

Förslag till direktiv
Artikel 8 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Samarbetsnätverket ska föra samman kommissionen och de ***behöriga myndigheterna*** i kontinuerlig kommunikation. På begäran ska ***Europeiska byrån för nät- och informationssäkerhet (***Enisa***)*** bistå samarbetsnätverket med expertis och råd.	2. Samarbetsnätverket ska föra samman kommissionen och de ***gemensamma kontaktpunkterna*** i kontinuerlig kommunikation. På begäran ska Enisa bistå samarbetsnätverket med expertis och råd. ***Vid behov får även marknadsoperatörer och leverantörer av it-säkerhetslösningar inbjudas att delta i verksamheten i det samarbetsnätverk som avses i punkt 3 g och i.*** ***Samarbetsnätverket ska, när så är lämpligt, samarbeta med dataskyddsmyndigheterna.*** ***Kommissionen ska regelbundet informera samarbetsnätverket om säkerhetsforskning och andra relevanta program inom Horisont 2020.***

Ändringsförslag 78

Förslag till direktiv
Artikel 8 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Inom samarbetsnätverket ska de ***behöriga myndigheterna*** göra följande:	3. Inom samarbetsnätverket ska de ***gemensamma kontaktpunkterna*** göra följande:
(a) Sprida tidiga varningar om risker och incidenter i enlighet med artikel 10.	(a) Sprida tidiga varningar om risker och incidenter i enlighet med artikel 10.
(b) Säkerställa samordnade svarsåtgärder i enlighet med artikel 11.	(b) Säkerställa samordnade svarsåtgärder i enlighet med artikel 11.
(c) Regelbundet offentliggöra ej konfidentiell information om pågående tidiga varningar och samordnade svarsåtgärder på en gemensam webbplats.	(c) Regelbundet offentliggöra ej konfidentiell information om pågående tidiga varningar och samordnade svarsåtgärder på en gemensam webbplats.
(d) ***På en begäran av en medlemsstat eller kommissionen*** gemensamt diskutera och bedöma en eller leda nationella NIS-strategier och nationella NIS-samarbetsplaner enligt artikel 5, inom detta direktivs räckvidd.	(d) Gemensamt diskutera och bedöma en eller leda nationella NIS-strategier och nationella NIS-samarbetsplaner enligt artikel 5, inom detta direktivs räckvidd.
(e) ***På begäran av en medlemsstat eller kommissionen*** gemensamt diskutera och bedöma incidenthanteringsorganisationernas effektivitet, i synnerhet när NIS-övningar genomförs på unionsnivå.	(e) Gemensamt diskutera och bedöma incidenthanteringsorganisationernas effektivitet, i synnerhet när NIS-övningar genomförs på unionsnivå.
(f) Samarbeta och utbyta ***information*** om ***alla*** relevanta frågor ***med Europeiska it-brottscentrumet inom Europol och med andra relevanta europeiska organ***, i synnerhet inom områdena dataskydd, energi, transport, bankverksamhet, ***börs*** och hälso- och sjukvård.	(f) Samarbeta och utbyta ***sakkunskap*** om relevanta frågor ***rörande nät- och informationssäkerhet***, i synnerhet inom områdena dataskydd, energi, transport, bankverksamhet, ***finansmarknader*** och hälso- och sjukvård***, med Europeiska it-brottscentrumet inom Europol och med andra relevanta europeiska organ***.
	(fa) Vid behov informera EU:s samordnare för kampen mot terrorism, genom en rapport, och eventuellt be denne om stöd i samband med samarbetsnätverkets analyser, förberedande arbeten och åtgärder.
(g) Utbyta information och bästa praxis med varandra och med kommissionen och bistå varandra i uppbyggnaden av NIS-kapacitet.	(g) Utbyta information och bästa praxis med varandra och med kommissionen och bistå varandra i uppbyggnaden av NIS-kapacitet.

(h) Anordna regelbundna kollegiala granskningar av kapacitet och beredskap.

(i) Anordna NIS-övningar på unionsnivå och delta, såsom lämpligt, i internationella NIS-övningar.	(i) Anordna NIS-övningar på unionsnivå och delta, såsom lämpligt, i internationella NIS-övningar.
	(ia) Involvera, samråda med och vid behov utbyta information med marknadsoperatörer med avseende på risker och incidenter som påverkar deras nät och informationssystem.
	(ib) I samarbete med Enisa utarbeta riktlinjer för sektorsspecifika kriterier för anmälan av betydande incidenter, utöver de faktorer som anges i artikel 14.2, i syfte att uppnå en gemensam tolkning, en enhetlig tillämpning och ett harmoniserat genomförande inom unionen.

Ändringsförslag 79

Förslag till direktiv
Artikel 8 – punkt 3a (ny)

Kommissionens förslag	*Ändringsförslag*
	3a. Samarbetsnätverket ska offentliggöra en årlig rapport som grundar sig på nätverkets verksamhet under de senaste tolv månaderna och på den sammanfattande rapport som ska lämnas in i enlighet med artikel 14.4 i detta direktiv.

Ändringsförslag 80

Förslag till direktiv
Artikel 8 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. Kommissionen ska genom genomförandeakter anta de bestämmelser som är nödvändiga för att underlätta samarbetet mellan ***behöriga myndigheter***	4. Kommissionen ska genom genomförandeakter anta de bestämmelser som är nödvändiga för att underlätta samarbetet mellan ***gemensamma***

och kommissionen enligt punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det ***samrådsförfarande*** som avses i artikel ***19.2***.

kontaktpunkter, kommissionen ***och Enisa*** enligt punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det ***granskningsförfarande*** som avses i artikel ***19.3***.

Ändringsförslag 81

Förslag till direktiv
Artikel 9 – punkt 1a (ny)

Kommissionens förslag	*Ändringsförslag*
	1a. Deltagare i den säkra infrastrukturen ska agera i överensstämmelse med bland annat lämpliga åtgärder för sekretess och säkerhet i enlighet med direktiv 95/46/EG och förordning (EG) nr 45/2001 under alla steg av behandlingen.

Ändringsförslag 82

Förslag till direktiv
Artikel 9 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 18 när det gäller definitionen av de kriterier som en medlemsstat ska uppfylla för att godkännas för deltagande i det säkra systemet för informationsutbyte, vad gäller följande:	***utgår***
(a) Medlemsstaten ska ha tillgång till en säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå, som ska vara förenlig och interoperabel med samarbetsnätverkets säkra infrastruktur i enlighet med artikel 7.3.	
(b) Den behöriga myndigheten och incidenthanteringsorganisationen ska ha tillräckliga tekniska och finansiella	

resurser samt personalresurser för att på ett effektivt och säkert sätt kunna delta i det säkra systemet för informationsutbyte i enlighet med artiklarna 6.3, 7.2 och 7.3.

Ändringsförslag 83

Förslag till direktiv
Artikel 9 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Kommissionen ska genom ***genomförandeakter besluta om medlemsstaternas tillträde till denna säkra infrastruktur, i enlighet med de kriterier som avses i punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.***	3. Kommissionen ska genom ***delegerade akter anta gemensamma standarder för samtrafik och säkerhet som de gemensamma kontaktpunkterna ska uppfylla innan de utbyter känslig och sekretessbelagd information inom samarbetsnätverket***.

Ändringsförslag 84

Förslag till direktiv
Artikel 10 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. De ***behöriga myndigheterna*** eller kommissionen ska lämna tidiga varningar inom samarbetsnätverket om de risker eller incidenter som uppfyller minst ett av följande villkor:	1. De ***gemensamma kontaktpunkterna*** eller kommissionen ska lämna tidiga varningar inom samarbetsnätverket om de risker eller incidenter som uppfyller minst ett av följande villkor:
(a) De ökar snabbt i omfattning eller kan öka snabbt i omfattning.	
(b) ***De överstiger*** eller ***kan*** överstiga den nationella kapaciteten för svarsåtgärder.	(b) ***Den gemensamma kontaktpunkten bedömer att risken*** eller ***incidenten skulle kunna*** överstiga den nationella kapaciteten för svarsåtgärder.
(c) De påverkar ***eller kan påverka*** mer än en medlemsstat.	(c) De ***gemensamma kontaktpunkterna eller kommissionen bedömer att risken eller incidenten*** påverkar mer än en medlemsstat.

Ändringsförslag 85

Förslag till direktiv
Artikel 10 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. I de tidiga varningarna ska de ***behöriga myndigheterna*** eller kommissionen meddela all relevant information som de förfogar över och som kan vara till nytta för att bedöma risken eller incidenten.	2. I de tidiga varningarna ska de ***gemensamma kontaktpunkterna*** eller kommissionen ***utan onödigt dröjsmål*** meddela all relevant information som de förfogar över och som kan vara till nytta för att bedöma risken eller incidenten.

Ändringsförslag 86

Förslag till direktiv
Artikel 10 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att en medlemsstat inkommer med relevant information om en specifik risk eller incident.	***utgår***

Ändringsförslag 87

Förslag till direktiv
Artikel 10 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. Om den risk eller incident som är föremål för en tidig varning misstänks vara av brottslig art ska ***de behöriga myndigheterna eller kommissionen underrätta*** Europeiska it-brottscentrumet inom Europol.	4. Om den risk eller incident som är föremål för en tidig varning misstänks vara av brottslig art ***och om den berörda marknadsoperatören har rapporterat incidenter som misstänks vara av allvarlig brottslig art enligt artikel 15.4*** ska ***medlemsstaterna i tillämpliga fall se till att*** Europeiska it-brottscentrumet inom Europol ***underrättas***.

Ändringsförslag 88

Förslag till direktiv
Artikel 10 – punkt 4a (ny)

Kommissionens förslag	*Ändringsförslag*
	4a. Medlemmarna i samarbetsnätverket får inte offentliggöra den mottagna informationen om risker och incidenter enligt punkt 1 utan att först ha erhållit godkännande från den anmälande gemensamma kontaktpunkten.
	Innan informationen utbyts inom samarbetsnätverket ska den anmälande gemensamma kontaktpunkten dessutom informera den marknadsoperatör som informationen avser om sin avsikt, och, i den mån den anser att det är lämpligt, anonymisera informationen.

Ändringsförslag 89

Förslag till direktiv
Artikel 10 – punkt 4b (ny)

Kommissionens förslag	*Ändringsförslag*
	4b. Om den risk eller incident som är föremål för en tidig varning misstänks vara av allvarlig gränsöverskridande teknisk art ska de gemensamma kontaktpunkterna eller kommissionen underrätta Enisa.

Ändringsförslag 90

Förslag till direktiv
Artikel 11 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Efter en tidig varning enligt artikel 10 ska de ***behöriga myndigheterna***, efter att gjort en bedömning av den relevanta informationen enas om samordnade	1. Efter en tidig varning enligt artikel 10 ska de ***gemensamma kontaktpunkterna***, efter att gjort en bedömning av den relevanta informationen ***och utan onödigt***

svarsåtgärder i enlighet med unionens NIS-samarbetsplan enligt artikel 12.	***dröjsmål,*** enas om samordnade svarsåtgärder i enlighet med unionens NIS-samarbetsplan enligt artikel 12.

Ändringsförslag 91

Förslag till direktiv
Artikel 12 – punkt 2 – led a – strecksats 1

Kommissionens förslag	*Ändringsförslag*
– En definition av format och förfaranden för de ***behöriga myndigheternas*** insamling och utbyte av kompatibla och jämförbara uppgifter om risker och incidenter.	– En definition av format och förfaranden för de ***gemensamma kontaktpunkternas*** insamling och utbyte av kompatibla och jämförbara uppgifter om risker och incidenter.

Ändringsförslag 92

Förslag till direktiv
Artikel 12 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Unionens NIS-samarbetsplan ska antas senast ett år efter detta direktivs ikraftträdande och regelbundet revideras.	3. Unionens NIS-samarbetsplan ska antas senast ett år efter detta direktivs ikraftträdande och regelbundet revideras. ***Resultaten av varje revidering ska rapporteras till Europaparlamentet.***

Ändringsförslag 93

Förslag till direktiv
Artikel 12 – punkt 3a (ny)

Kommissionens förslag	*Ändringsförslag*
	3a. Det ska säkerställas att det råder samstämdhet mellan unionens NIS-samarbetsplan och de nationella NIS-strategier och NIS-samarbetsplaner som föreskrivs i artikel 5 i detta direktiv.

Ändringsförslag 94

Förslag till direktiv
Artikel 13 – punkt 1

Kommissionens förslag	*Ändringsförslag*
Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. Sådana avtal ska beakta behovet av ändamålsenligt skydd för personuppgifter som förmedlas via samarbetsnätverket.	Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. Sådana avtal ska beakta behovet av ändamålsenligt skydd för personuppgifter som förmedlas via samarbetsnätverket ***samt ange det kontrollförfarande som ska tillämpas för att garantera skyddet av sådana personuppgifter***. ***Europaparlamentet ska informeras om avtalsförhandlingarna. Om personuppgifter överförs till mottagare i länder utanför unionen ska det ske i enlighet med artiklarna 25 och 26 i direktiv 95/46/EG och artikel 9 i förordning (EG) nr 45/2001.***

Ändringsförslag 95

Förslag till direktiv
Artikel 13a (ny)

Kommissionens förslag	*Ändringsförslag*
	Artikel 13a
	Marknadsoperatörernas kritikalitet
	Medlemsstaterna får fastställa marknadsoperatörernas kritikalitet, med hänsyn till de särskilda förhållandena i sektorn, faktorer såsom den berörda marknadsoperatörens betydelse för att upprätthålla en tillräcklig service i sektorn, antalet parter som marknadsoperatören levererar tjänster till

och den tid det tar innan avbrottet i marknadsoperatörens kärntjänster får en negativ inverkan på upprätthållandet av viktig ekonomisk och samhällelig verksamhet.

Motivering

Detta ändringsförslag är en del av kapitel IV och bör placeras före artikel 14. Syftet med denna artikel är att öppna för en mer differentierad klassificering i bilaga II och därmed av de skyldigheter som anges i kapitel IV. Alla marknadsoperatörer ska anmäla incidenter oavsett hur kritiska de är, medan utformningen av säkerhetsrevisioner får anpassas efter marknadsoperatörens specifika kritikalitet.

Ändringsförslag 96

Förslag till direktiv
Artikel 14 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Medlemsstaterna ska se till att ***offentliga förvaltningar och*** marknadsoperatörer vidtar ändamålsenliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten för de nät och informationssystem som de kontroller och använder i sin verksamhet. Med beaktande av den senaste tekniken ska dessa åtgärder garantera en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga och minimera de effekter som incidenter som påverkar deras nät och informationssystem har på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem.	1. Medlemsstaterna ska se till att marknadsoperatörer vidtar ändamålsenliga ***och proportionerliga*** tekniska och organisatoriska åtgärder för att ***upptäcka och effektivt*** hantera risker som hotar säkerheten för de nät och informationssystem som de kontrollerar och använder i sin verksamhet. Med beaktande av den senaste tekniken ska dessa åtgärder garantera en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga och minimera de effekter som incidenter som påverkar ***säkerheten för*** deras nät och informationssystem har på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem.

Ändringsförslag 97

Förslag till direktiv
Artikel 14 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Medlemsstaterna ska säkerställa att ***offentliga förvaltningar och*** marknadsoperatörer underrättar den behöriga myndigheten om incidenter som har en betydande inverkan på ***säkerheten*** för de kärntjänster som de tillhandahåller.	2. Medlemsstaterna ska säkerställa att marknadsoperatörer ***utan onödigt dröjsmål*** underrättar den behöriga myndigheten ***eller den gemensamma kontaktpunkten*** om incidenter som har en betydande inverkan på ***kontinuiteten*** för de kärntjänster som de tillhandahåller. ***Anmälan ska inte medföra ökad ansvarsskyldighet för den anmälande parten.*** ***För att avgöra om en incident har en betydande inverkan ska man ta hänsyn till bl.a. följande faktorer:***

Ändringsförslag 98

Förslag till direktiv
Artikel 14 – punkt 2 – led a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(a) Hur många användares kärntjänster som påverkas.

Ändringsförslag 99

Förslag till direktiv
Artikel 14 – punkt 2 – led b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(b) Hur länge incidenten varar.

Ändringsförslag 100

Förslag till direktiv
Artikel 14 – punkt 2 – led c (nytt)

Kommissionens förslag	*Ändringsförslag*
	(c) Hur stort geografiskt område som påverkas av incidenten.

Ändringsförslag 101

Förslag till direktiv
Artikel 14 – punkt 2 – stycke 1a (nytt)

Kommissionens förslag	*Ändringsförslag*
	Dessa faktorer ska anges närmare enligt artikel 8.3 ib.

Ändringsförslag 102

Förslag till direktiv
Artikel 14 – punkt 2a (ny)

Kommissionens förslag	*Ändringsförslag*
	2a. Marknadsoperatörerna ska anmäla de incidenter som avses i punkterna 1 och 2 till den behöriga myndigheten eller den gemensamma kontaktpunkten i den medlemsstat där kärntjänsten påverkas. Om kärntjänster påverkas i mer än en medlemsstat, ska den gemensamma kontaktpunkt som har mottagit anmälan meddela övriga berörda gemensamma kontaktpunkter med utgångspunkt i informationen från marknadsoperatören. Marknadsoperatörer ska så snart som möjligt få veta vilka andra gemensamma kontaktpunkter som underrättats om incidenten, samt om eventuella vidtagna åtgärder, resultat och all annan information av relevans för incidenten.

Ändringsförslag 103

Förslag till direktiv
Artikel 14 – punkt 2b (ny)

Kommissionens förslag	*Ändringsförslag*
	2b. Om anmälan innehåller personuppgifter ska den lämnas ut enbart

	till mottagare inom den underrättade behöriga myndigheten eller gemensamma kontaktpunkten vilka behöver behandla uppgifterna i fråga för att kunna utföra sina uppdrag i enlighet med dataskyddsbestämmelserna. De uppgifter som lämnas ut ska begränsas till vad som är nödvändigt för att dessa personer ska kunna utföra sina uppdrag.

Ändringsförslag 104

Förslag till direktiv
Artikel 14 – punkt 2c (ny)

Kommissionens förslag	*Ändringsförslag*
	2c. Marknadsoperatörer som inte omfattas av bilaga II får på frivillig basis rapportera incidenter av det slag som anges i artikel 14.2.

Ändringsförslag 105

Förslag till direktiv
Artikel 14 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. Den behöriga myndigheten får informera allmänheten ***eller kräva att de offentliga myndigheterna och marknadsoperatörerna informerar allmänheten***, om den ***fastställer*** att ***det ligger i allmänhetens intresse*** att incidenten ***röjs***. En gång om året ska den ***behöriga myndigheten*** lämna in en sammanfattande rapport till samarbetsnätverket om de anmälningar som kommit in och de åtgärder som vidtagits i enlighet med denna punkt.	4. ***Efter samråd med*** den ***underrättade*** behöriga myndigheten ***och den berörda marknadsoperatören*** får ***den gemensamma kontaktpunkten*** informera allmänheten ***om enskilda incidenter***, om den ***bedömer*** att ***allmänheten behöver känna till dessa för*** att ***man ska kunna förhindra en incident eller åtgärda en pågående incident eller om den marknadsoperatör som drabbats av en incident har avböjt att utan onödigt dröjsmål åtgärda en allvarlig strukturell sårbarhet i samband med den*** incidenten. ***Innan information lämnas ut till allmänheten ska den underrättade behöriga myndigheten se till att den***

	berörda marknadsoperatören ges tillfälle att höras och att beslutet om att lämna ut information till allmänheten är välavvägt i förhållande till allmänhetens intresse.
	Om information om enskilda incidenter offentliggörs ska den underrättade behöriga myndigheten eller gemensamma kontaktpunkten se till att informationen är så anonymiserad som möjligt.
	Den behöriga myndigheten eller den gemensamma kontaktpunkten ska, om det är rimligen möjligt, ge den berörda marknadsoperatören information som möjliggör en effektiv hantering av den anmälda incidenten.
	En gång om året ska den ***gemensamma kontaktpunkten*** lämna in en sammanfattande rapport till samarbetsnätverket om de anmälningar som kommit in ***– inklusive antalet anmälningar och med avseende på de incidentfaktorer som anges i punkt 2 i denna artikel –*** och de åtgärder som vidtagits i enlighet med denna punkt.

Ändringsförslag 106

Förslag till direktiv
Artikel 14 – punkt 4a (ny)

Kommissionens förslag	*Ändringsförslag*
	4a. Medlemsstaterna ska uppmuntra marknadsoperatörer att på frivillig basis offentliggöra incidenter som involverar deras företag i sina redovisningar.

Ändringsförslag 107

Förslag till direktiv
Artikel 14 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet artikel 18 när det gäller definition av de omständigheter då offentliga förvaltningar och marknadsoperatörer är skyldiga att anmäla incidenter.	***utgår***

Ändringsförslag 108

Förslag till direktiv
Artikel 14 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. ***Utan att det påverkar tillämpningen av delegerade akter som antas enligt punkt 5 får*** de behöriga myndigheterna anta riktlinjer ***och, om nödvändigt, utfärda anvisningar*** avseende de omständigheter då ***offentliga förvaltningar och*** marknadsoperatörer är skyldiga att anmäla incidenter.	6. De behöriga myndigheterna ***eller den gemensamma kontaktpunkten får*** anta riktlinjer avseende de omständigheter då marknadsoperatörer är skyldiga att anmäla incidenter.

Ändringsförslag 109

Förslag till direktiv
Artikel 14 – punkt 8

Kommissionens förslag	*Ändringsförslag*
8. Punkterna 1 och 2 ska inte tillämpas på mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag[12].	8. Punkterna 1 och 2 ska inte tillämpas på mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag[12]***, såvida inte mikroföretaget är ett dotterbolag till en marknadsoperatör enligt definitionen i artikel 3 8 b***.
[12] EUT L 124, 20.5.2003, s. 36.	[12] EUT L 124, 20.5.2003, s. 36.

Ändringsförslag 110

Förslag till direktiv
Artikel 14 – punkt 8a (ny)

Kommissionens förslag	*Ändringsförslag*
	8a. Medlemsstaterna får besluta att tillämpa denna artikel och artikel 15 på offentliga förvaltningar i tillämpliga delar.

Ändringsförslag 111

Förslag till direktiv
Artikel 15 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter de behöver för att ***utreda fall då offentliga förvaltningar eller*** marknadsoperatörer ***inte uppfyllt*** sina skyldigheter enligt artikel 14 ***och*** de effekter som detta har på nätens och informationssystemens säkerhet.	1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har de befogenheter de behöver för att ***säkerställa att*** marknadsoperatörer ***uppfyller*** sina skyldigheter enligt artikel 14***, med*** de effekter som detta har på nätens och informationssystemens säkerhet.

Ändringsförslag 112

Förslag till direktiv
Artikel 15 – punkt 2 – inledningen

Kommissionens förslag	*Ändringsförslag*
2. Medlemsstaterna ska se till att de behöriga myndigheterna har befogenhet att ålägga att marknadsoperatörer ***och offentliga förvaltningar***	2. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har befogenhet att ålägga att marknadsoperatörer

Ändringsförslag 113

Förslag till direktiv
Artikel 15 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) ***genomgår*** en säkerhetsrevision som utförs av ett kvalificerat oberoende organ eller av en nationell myndighet och ***ge*** den behöriga myndigheten tillgång till ***resultaten***.	(b) ***tillhandahåller dokumentation som visar att säkerhetsåtgärderna genomförts effektivt, t.ex. resultaten av*** en säkerhetsrevision som utförs av ett kvalificerat oberoende organ eller av en nationell myndighet***,*** och ***ger*** den behöriga myndigheten ***eller den gemensamma kontaktpunkten*** tillgång till ***dokumentationen***.

Ändringsförslag 114

Förslag till direktiv
Artikel 15 – punkt 2 – stycke 1a (nytt)

Kommissionens förslag	*Ändringsförslag*
	I en sådan begäran ska de behöriga myndigheterna och de gemensamma kontaktpunkterna uppge syftet med begäran och ange tillräckligt tydligt vilken information som begärs.

Ändringsförslag 115

Förslag till direktiv
Artikel 15 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Medlemsstaterna ska se till att de behöriga myndigheterna har befogenhet att utfärda bindande anvisningar för marknadsoperatörer ***och offentliga förvaltningar***.	3. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har befogenhet att utfärda bindande anvisningar för marknadsoperatörer.

Ändringsförslag 116

Förslag till direktiv
Artikel 15 – punkterna 3a and 3b (nya)

Kommissionens förslag	*Ändringsförslag*
	3a. Genom undantag från punkt 2 b i denna artikel får medlemsstaterna besluta att de behöriga myndigheterna eller de gemensamma kontaktpunkterna i förekommande fall ska tillämpa ett annat förfarande på vissa marknadsoperatörer, baserat på deras kritikalitet, fastställd i enlighet med artikel 13a. Om medlemsstaterna fattar ett sådant beslut gäller följande:
	(a) De behöriga myndigheterna eller i förekommande fall den gemensamma kontaktpunkten ska ha behörighet att rikta en tillräckligt specifik begäran till marknadsoperatörerna och kräva att de tillhandahåller dokumentation som visar att säkerhetsåtgärderna genomförts effektivt, t.ex. resultaten av en säkerhetsrevision som utförs av en kvalificerad internrevisor, och ger den behöriga myndigheten eller den gemensamma kontaktpunkten tillgång till dokumentationen.
	(b) När marknadsoperatören har gjort den begäran som avses i led a får den behöriga myndigheten eller den gemensamma kontaktpunkten vid behov begära ytterligare dokumentation eller kräva att en ytterligare revision utförs av ett kvalificerat oberoende organ eller av en nationell myndighet.
	3b. Medlemsstaterna får besluta att minska antalet revisioner och intensiteten i dessa för en berörd marknadsoperatör om den säkerhetsrevision som operatören varit föremål för konsekvent visar på överensstämmelse med kapitel IV.

Ändringsförslag 117

Förslag till direktiv
Artikel 15 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. De behöriga myndigheterna ska anmäla incidenter som misstänks vara av allvarlig brottslig art till de rättsvårdande myndigheterna.	4. De behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ska ***informera de berörda marknadsoperatörerna om möjligheten att*** anmäla incidenter som misstänks vara av allvarlig brottslig art till de rättsvårdande myndigheterna.

Ändringsförslag 118

Förslag till direktiv
Artikel 15 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. De behöriga myndigheterna ***ska*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott.	5. ***Utan att det påverkar tillämpliga dataskyddsregler ska*** de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott. ***De gemensamma kontaktpunkterna och dataskyddsmyndigheterna ska i samarbete med Enisa utforma mekanismer för informationsutbyte och en gemensam mall för anmälningar både enligt artikel 14.2 i detta direktiv och enligt annan unionslagstiftning om dataskydd.***

Ändringsförslag 119

Förslag till direktiv
Artikel 15 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. Medlemsstaterna ska säkerställa att alla skyldigheter som införs för ***offentliga förvaltningar och*** marknadsoperatörer i enlighet med detta kapitel kan bli föremål för rättslig prövning.	6. Medlemsstaterna ska säkerställa att alla skyldigheter som införs för marknadsoperatörer i enlighet med detta kapitel kan bli föremål för rättslig prövning.

Ändringsförslag 120

Förslag till direktiv
Artikel 15 – punkt 6a (ny)

Kommissionens förslag	*Ändringsförslag*
	6a. Medlemsstaterna får besluta att tillämpa artikel 14 och denna artikel på offentliga förvaltningar i tillämpliga delar.

Ändringsförslag 121

Förslag till direktiv
Artikel 16 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. För att säkerställa en enhetlig tillämpning av artikel 14.1 ska medlemsstaterna främja användningen av standarder och/eller specifikationer av relevans för nät- och informationssäkerheten.	1. För att säkerställa en enhetlig tillämpning av artikel 14.1 ska medlemsstaterna***, utan att föreskriva användning av särskild teknik,*** främja användningen av ***interoperabla europeiska eller internationella*** standarder och/eller specifikationer av relevans för nät- och informationssäkerheten.

Ändringsförslag 122

Förslag till direktiv
Artikel 16 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Kommissionen ska ***i genomförandeakter*** utarbeta en lista över de standarder som avses i punkt 1. Listan ska kungöras i Europeiska unionens officiella tidning.	2. Kommissionen ska ***uppdra åt ett relevant europeiskt standardiseringsorgan att under samråd med relevanta aktörer*** utarbeta en lista över de standarder ***och/eller specifikationer*** som avses i punkt 1. Listan ska kungöras i Europeiska unionens officiella tidning.

Ändringsförslag 123

Förslag till direktiv
Artikel 17 – punkt 1a (ny)

Kommissionens förslag	*Ändringsförslag*
	1a. Medlemsstaterna ska se till att de påföljder som avses i punkt 1 i denna artikel är tillämpliga endast om en marknadsoperatör avsiktligt eller till följd av allvarlig försumlighet har underlåtit att fullgöra sina skyldigheter enligt kapitel IV.

Ändringsförslag 124

Förslag till direktiv
Artikel 18 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Den delegering av befogenhet som avses i ***artiklarna 9.2, 10.5 and 14.5*** får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i Europeiska unionens officiella tidning, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.	3. Den delegering av befogenhet som avses i ***artikel 9.2*** får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i Europeiska unionens officiella tidning, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

Ändringsförslag 125

Förslag till direktiv
Artikel 18 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. En delegerad akt som antas i enlighet med ***artiklarna 9.2, 10.5 och 14.5*** ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten	5. En delegerad akt som antas i enlighet med ***artikel 9.2*** ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från

inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.	den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Ändringsförslag 126

Förslag till direktiv
Artikel 20

Kommissionens förslag	*Ändringsförslag*
Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast tre år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.	Kommissionen ska regelbundet se över hur detta direktiv fungerar***, i synnerhet listan i bilaga II,*** och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast tre år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.

Ändringsförslag 127

Förslag till direktiv
Bilaga 1 – rubrik 1

Kommissionens förslag	*Ändringsförslag*
Krav och uppgifter för ***incidenthanteringsorganisationen*** (Cert)	Krav och uppgifter för ***incidenthanteringsorganisationerna*** (Cert)

Ändringsförslag 128

Förslag till direktiv
Bilaga 1 – led 1 – led a

Kommissionens förslag	*Ändringsförslag*
(a) ***Incidenthanteringsorganisationen*** ska säkerställa god tillgång till sina kommunikationstjänster genom att undvika felkritiska systemdelar (single points of failure) och kunna kontaktas och kontakta andra på flera olika sätt. Kommunikationskanalerna ska vara tydligt specificerade och välkända för användargruppen och samarbetspartner.	(a) ***Incidenthanteringsorganisationerna*** ska säkerställa god tillgång till sina kommunikationstjänster genom att undvika felkritiska systemdelar (single points of failure) och ***alltid*** kunna kontaktas och kontakta andra på flera olika sätt. Kommunikationskanalerna ska vara tydligt specificerade och välkända för användargruppen och samarbetspartner.

Ändringsförslag 129

Förslag till direktiv
Bilaga 1 – led 1 – led c

Kommissionens förslag	*Ändringsförslag*
(c) ***Incidenthanteringsorganisationens*** kontor och de informationssystem som ***den*** använder sig av ska vara lokaliserade till säker plats.	(c) ***Incidenthanteringsorganisationernas*** kontor och de informationssystem som ***de*** använder sig av ska vara lokaliserade till säker plats ***med säkra nät och informationssystem***.

Ändringsförslag 130

Förslag till direktiv
Bilaga 1 – led 2 – led a – strecksats 1

Kommissionens förslag	*Ändringsförslag*
– Övervakning av incidenter på nationell nivå.	– ***Upptäckt och*** övervakning av incidenter på nationell nivå.

Ändringsförslag 131

Förslag till direktiv
Bilaga 1 – led 2 – led a – strecksats 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	– Aktivt deltagande i samarbetsnätverk för incidenthanteringsorganisationer på EU-

	nivå och internationell nivå.

Ändringsförslag 132

Förslag till direktiv
Bilaga II – inledningen

Kommissionens förslag	*Ändringsförslag*
Lista över marknadsoperatörer	Lista över marknadsoperatörer
Enligt artikel 3.8 a:	
1. E-handelsplattformar.	
2. Internetbetalningsslussar.	
3. Sociala medier.	
4. Sökmotorer	
5. Molntjänster.	
6. Onlineförsäljning av tillämpningar.	
Enligt artikel 3.8 b	

Ändringsförslag 133

Förslag till direktiv
Bilaga II – led 1

Kommissionens förslag	*Ändringsförslag*
Lista över marknadsoperatörer	Lista över marknadsoperatörer
1. Energi.	1. Energi.
	(a) Elektricitet.
– ***El- och gasleverantörer***.	– ***Leverantörer***.
– Systemansvariga för ***el- och/eller gasdistributionssystem*** och återförsäljare till slutkunderna.	– Systemansvariga för ***distributionssystem*** och återförsäljare till slutkunderna.
– Systemansvariga för gasöverföringssystem, naturgaslager och LNG.	
– Systemansvariga för elöverföringssystem.	– Systemansvariga för elöverföringssystem.
	(b) Olja.

– Oljeledningar och oljelager.	– Oljeledningar och oljelager.
	– Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring.
	(c) Gas.
– ***El- och gasmarknadsaktörer***.	– ***Leverantörer***.
	– Systemansvariga för distributionssystem och återförsäljare till slutkunderna.
	– Systemansvariga för gasöverföringssystem, naturgaslager och LNG.
– Operatörer av ***olje- och*** naturgasproduktion, raffinaderier och ***bearbetningsanläggningar***.	– Operatörer av naturgasproduktion, raffinaderier***, bearbetningsanläggningar, lagring*** och ***överföring***.
	– Gasmarknadsoperatörer.

Ändringsförslag 134

Förslag till direktiv
Bilaga II – led 2

Kommissionens förslag	*Ändringsförslag*
2. Transporter.	2. Transporter.
– Lufttrafikföretag (gods- och persontransporter).	***(a) Vägtransport***
– Sjötransportföretag (transportföretag som bedriver persontrafik till havs och längs kuster samt transportföretag som bedriver godstrafik till havs och längs kuster).	***(i) Trafikstyrning och trafikledning***.
– Järnväg (infrastrukturförvaltare, integrerade företag och järnvägstransportföretag).	***(ii) Logistiska stödtjänster:***
– ***Flygplatser***.	– ***Lager- och magasineringstjänster***.
– ***Hamnar***	– ***Godshantering.***
– ***Trafikstyrning och trafikledning***.	– ***Andra stödverksamheter för transporter***.
– Logistiska stödtjänster a) lager- och magasineringstjänster, b) godshantering och c) andra stödverksamheter för	***(b) Järnvägstransport***

transporter).

(i) Järnväg (infrastrukturförvaltare, integrerade företag och järnvägstransportföretag).

(ii) Trafikstyrning och trafikledning.

(iii) Logistiska stödtjänster:

– Lager- och magasineringstjänster.

– Godshantering.

– Andra stödverksamheter för transporter.

(c) Luftfart.

(i) Lufttrafikföretag (gods- och persontransporter).

(ii) Flygplatser.

(iii) Trafikstyrning och trafikledning.

(iv) Logistiska stödtjänster:

– Lagertjänster.

– Godshantering.

– Andra stödverksamheter för transporter.

(d) Sjötransporter.

(i) Sjötransportföretag (transportföretag som bedriver persontrafik på inre vattenvägar, till havs och längs kuster samt transportföretag som bedriver godstrafik på inre vattenvägar, till havs och längs kuster).

Ändringsförslag 135

Förslag till direktiv
Bilaga II – led 4

Kommissionens förslag	*Ändringsförslag*
4. Finansmarknadsinfrastruktur: ***börser*** och organisationer för central motpartsclearing.	4. Finansmarknadsinfrastruktur: ***reglerade marknader, multilaterala handelsplattformar, organiserade handelsplattformar*** och organisationer för central motpartsclearing.

Ändringsförslag 136

Förslag till direktiv
Bilaga II – led 5a (nytt)

Kommissionens förslag	*Ändringsförslag*
	5a. Vattenproduktion och vattenförsörjning.

Ändringsförslag 137

Förslag till direktiv
Bilaga II – led 5b (nytt)

Kommissionens förslag	*Ändringsförslag*
	5b. Försörjningskedjan för livsmedel.

Ändringsförslag 138

Förslag till direktiv
Bilaga II – led 5c (nytt)

Kommissionens förslag	*Ändringsförslag*
	5c. Internetknutpunkter.

MOTIVERING

1. Bakgrund

Redan 2010 i den digitala agendan för Europa efterlystes lagstiftning för en politik för nät- och informationssäkerhet på hög nivå. Eftersom nät- och informationssystemen är sammanlänkade kan allvarliga systemstörningar i en medlemsstat påverka andra medlemsstater och unionen som helhet. Tillförlitlighet och stabilitet i nät- och informationssystem samt kontinuitet i kärntjänsterna är en förutsättning för en välfungerande inre marknad, särskilt för den digitala inre marknadens fortsatta utveckling.

Bakgrunden till Europeiska kommissionens föreliggande förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen är de olika kapacitetsnivåerna och fragmenteringen i unionen. Förslaget syftar till att förbättra säkerheten på internet och i de privata nät- och informationssystem som stöder funktionerna i våra samhällen och ekonomier.

Kommissionen uppmanar därför medlemsstaterna att öka beredskapen och förbättra samarbetet med varandra. För detta ändamål bör operatörer av kritisk infrastruktur inom områden som energi, transport, och viktiga leverantörer av informationssamhällets tjänster, liksom offentliga förvaltningar, vidta ändamålsenliga åtgärder för att hantera säkerhetsrisker och rapportera allvarliga incidenter till de behöriga nationella myndigheterna.

2. Förslag till betänkande

Föredraganden stöder det föreslagna direktivets övergripande syfte, dvs. att säkerställa en hög gemensam nivå av nät- och informationssäkerhet. För att öka effektiviteten i de föreslagna åtgärderna anser föredraganden att detta direktiv till att börja med bör begränsas till vissa operatörer, säkerställa de investeringar i nät- och informationssäkerhet som redan är gjorda och förhindra dubblering av institutionella strukturer och av de skyldigheter som ålagts marknadsoperatörerna. Föredraganden anser dessutom att detta direktiv bör främja utveckling av ömsesidigt förtroende och utbyte mellan offentliga och privata aktörer samt förhindra ogynnsamma reaktioner i form av en ”efterlevnadskultur” i stället för en önskvärd ”riskhanteringskultur”. Mot bakgrund av dessa aspekter föreslår föredraganden att man stärker direktivets verkan genom följande huvudsakliga ändringar.

A. Räckvidd

Förslaget till direktiv syftar till att ålägga offentliga förvaltningar och marknadsoperatörer skyldigheter när det gäller bl.a. kritiska infrastrukturer och informationssamhällets tjänster. För att direktivet ska ge proportionalitet och snabba resultat anser föredraganden att de obligatoriska åtgärder som fastställs i kapitel IV bör begränsas till infrastrukturer som är kritiska i striktare bemärkelse. Föredraganden anser att informationssamhällets tjänster därför inte bör ingå i bilaga II till detta direktiv. Direktivet bör i stället inriktas på

marknadsoperatörer som tillhandahåller tjänster, bl.a. inom energi- och transportsektorn samt inom hälso- och sjukvårdsrelaterad infrastruktur och finansmarknadsinfrastrukturer.

Med tanke på det allmännyttiga uppdraget måste offentliga förvaltningar förvalta sina nät- och informationssystem med vederbörlig aktsamhet. Föredraganden anser därför inte att det är rimligt att dessa åläggs samma skyldigheter som marknadsoperatörer och föreslår således ändrad räckvidd.
Vid sidan om detta håller föredraganden med om att bilaga II bör ha en ej uttömmande karaktär och att direktivet bör ses över med jämna mellanrum, även med hänsyn till utvecklingen av ny teknik.

B. Nationella behöriga myndigheter

I förslaget till direktiv föreskrivs att varje medlemsstat ska utse en nationell behörig myndighet som ansvarar för att övervaka tillämpningen av direktivet. Föredraganden anser att man med denna bestämmelse inte tar tillräcklig hänsyn till befintliga strukturer.
Inom vissa av de sektorer som omfattas av direktivet rapporterar marknadsoperatörerna redan formellt eller informellt vissa nät- och informationssäkerhetsincidenter till de sektorsspecifika tillsynsmyndigheterna. Dessa myndigheter har direkt koppling och nära förbindelse till respektive sektor och därmed ingående kunskaper om hot och sårbarhet, särskilt inom den egna sektorn, och har därför unika möjligheter att bedöma effekterna av potentiella och inträffade incidenter inom sektorn.

Utöver befintliga sektorsinvesteringar kan vissa medlemsstater behöva utse mer än en nationell behörig myndighet på grund av sin konstitutionella struktur eller andra omständigheter. Därför föreslår föredraganden att direktivet ändras så att varje medlemsstat kan utse mer än en behörig myndighet. För att säkerställa enhetlig tillämpning inom medlemsstaten och för att möjliggöra ett effektivt och smidigt samarbete på unionsnivå bör varje medlemsstat utse en gemensam kontaktpunkt som ansvarar för bl.a. deltagandet i samarbetsnätverket enligt artikel 8 och tidiga varningar i enlighet med artikel 10.

C. Samarbetsnätverk

För att stärka samarbetsnätverkets verksamhet anser föredraganden att man bör överväga att inbjuda marknadsoperatörer att delta när så är lämpligt. Dessutom skulle en årsrapport om nätverkets verksamhet ge värdefull information om hur utbytet av bästa metoder förlöper mellan medlemsstaterna och hur incidentrapporteringen utvecklas i unionen.

D. Säkerhetskrav och anmälan av incidenter

Den främsta nyheten i förslaget till direktiv är införandet av en skyldighet för marknadsoperatörer att rapportera incidenter som har en betydande inverkan på säkerheten för de kärntjänster som de tillhandahåller. För att klargöra skyldigheternas omfattning och införliva dem i den grundläggande akten föreslår föredraganden att de delegerade akterna enligt artikel 14.5 ersätts med tydliga kriterier för huruvida en incident har en betydande inverkan och ska anmälas. Med tanke på avsikten att skapa överensstämmelse med

direktiv 2009/140/EG skulle omfattningen av och kriterierna för anmälan kunna klargöras med hjälp av indikatorer liknande dem som fastställs i Enisas tekniska riktlinjer för incidentrapportering i samband med direktiv 2009/140/EG. Föredraganden rekommenderar också att man stärker skyddet när det gäller offentliggörande av information i samband med incidenter och klargör lagstiftningens tillämplighet i det fall en incident påverkar kärntjänsterna i flera medlemsstater, så att det inte införs ett flertal eller oklara rapporteringsskyldigheter.

E. Genomförande och efterlevnad

Föredraganden anser att man måste främja en riskhanteringskultur och bygga vidare på marknadsoperatörernas befintliga ansträngningar. I detta sammanhang är formen för tillhandahållandet av information om den konkreta riskhanteringen inte det viktigaste, utan snarare det övergripande samarbetet och de konkreta åtgärder som marknadsoperatörerna vidtar.

Artikel 15 måste därför ge utrymme för flexibilitet när det gäller dokumentationen om efterlevnad av de säkerhetskrav som införs för marknadsoperatörer. Det bör vara tillåtet att intyga efterlevnad på annat sätt än genom säkerhetsrevisioner.

F. Påföljder

Visserligen behövs påföljder för marknadsoperatörer vid överträdelser för att stärka direktivets effektivitet, men föredraganden anser att potentiella påföljder inte bör avskräcka från att rapportera incidenter och ge negativa effekter. Man bör förhindra att snabb incidentrapportering motverkas av risken för påföljder för bl.a. blotta överträdelsen av formföreskrifter. Föredraganden föreslår därför ett klargörande om att ingen påföljd bör fastställas om marknadsoperatören oavsiktligt eller utan stor försumlighet har underlåtit att fullgöra skyldigheterna enligt kapitel IV.

19.12.2013

YTTRANDE FRÅN UTSKOTTET FÖR INDUSTRIFRÅGOR, FORSKNING OCH ENERGI(*)

till utskottet för den inre marknaden och konsumentskydd

över förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Föredragande(*): Pilar del Castillo Vera

(*) Förfarande med associerat utskott – artikel 50 i arbetsordningen

KORTFATTAD MOTIVERING

Efter en begäran från Europaparlamentet i dess initiativbetänkande om en digital agenda för Europa lade Europeiska kommissionen i februari 2013 fram ett förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, tillsammans med EU:s första strategi för it-säkerhet. En analys av tillgängliga uppgifter leder till uppskattningen att skadliga IKT-relaterade incidenter kan orsaka direkta kostnader på över 560 miljoner euro per år, enbart för små och medelstora företag, och att alla typer av incidenter (inklusive miljömässiga eller fysiska problem som naturkatastrofer i föregående led) kan orsaka direkta kostnader på över 2,3 miljarder euro. Föredraganden rekommenderar därför varmt förslaget.

När det gäller konstruktionen instämmer föredraganden i ett antal av de föreslagna åtgärderna, såsom att utvidga bestämmelserna om att rapportera säkerhetsincidenter, vilka för närvarande begränsas till telekommunikationsleverantörer enligt artikel 13a i 2009 års ramdirektiv, till andra viktiga infrastruktursektorer. Förslag som att kräva att alla medlemsstater måste ha korrekt fungerande incidenthanteringsorganisationer, och utse en behörig myndighet som ska ingå i ett säkert alleuropeiskt nät för elektroniskt datautbyte för att möjliggöra säker delning och utbyte av it-säkerhetsrelaterad information, mottas väl och har goda möjligheter att i stor utsträckning bidra till det föreslagna direktivets målsättning, nämligen att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen.

Föredraganden anser emellertid att det finns utrymme för att förbättra förslaget genom att tillämpa två huvudprinciper: effektivitet och tillit.

Första principen – effektivitet

När det gäller medlemsstaternas skyldigheter att utse en behörig myndighet som ansvarar för att övervaka tillämpningen av direktivet för alla sektorer i bilaga II till förslaget, anser föredraganden att varje medlemsstat inte bara bör ha rätt att välja den modell för förvaltning av it-strategi som den bedömer som lämpligast, utan även att det är nödvändigt att undvika dubbla institutionella strukturer som riskerar att leda till behörighetskonflikter och kommunikationsavbrott. Föredraganden anser därför att befintliga nationella strukturer som redan fungerar effektivt och motsvarar medlemsstaternas behov och konstitutionella krav inte bör avbrytas. Hon anser emellertid att för att garantera informationsutbytet på unionsnivå, anmälan av tidiga varningar och ett effektivt deltagande i samarbetsnätverket måste varje medlemsstat utnämna en **central kontaktpunkt**.

På samma sätt, och för att det föreslagna direktivet ska bli så effektivt som möjligt, anser föredraganden att de föreslagna åtgärderna rörande inrättandet av en nationell **incidenthanteringsorganisation** (Computer Emergency Response Team, Cert) kanske inte visar sig vara det lämpligaste kravet, med tanke på att man då bortser från befintliga cert-organisationers olika typer och sammansättningar. Flertalet medlemsstater har fler än en cert och de hanterar också olika typer av incidenter. Verksamhetens kvantitet och kvalitet skiljer sig också åt, beroende på om det är akademiska institutioner eller forskningsinstitut, regeringar eller den privata sektorn som ansvarar för och driver dem. Dessutom skulle det aktuella förslaget störa existerande internationella och europeiska samarbetsnätverk, som befintliga cert redan tillhör, vilka har visat sig effektiva när det gäller att samordna internationella och europeiska insatser mot incidenter. Föredraganden anser därför att i stället för att hänvisa till en enda nationell cert bör direktivet inriktas på de cert som erbjuder sina tjänster till sektorerna inom Bilaga II, vilket innebär att en cert erbjuder tjänster till alla sektorer inom Bilaga II eller att flera cert erbjuder tjänster till samma sektor. Föredraganden anser emellertid att medlemsstaterna hela tiden måste garantera fullständig driftsäkerhet för sina cert och även garantera att de har tillräckliga tekniska, ekonomiska och personalmässiga resurser för att korrekt driva och delta i nätverk för samarbete både internationellt och på unionsnivå.

Effektivitetsprincipen kräver dessutom förändringar i det föreslagna direktivet när det gäller **tillämpningsområdet**. Även om föredraganden instämmer i att rapporteringssystemets skyldigheter behöver utvidgas till energi-, transport-, hälso- och ekonomisektorerna, är förslaget att utvidga de obligatoriska åtgärderna i kapitel IV till alla marknadsaktörer inom ”internetekonomin” oproportionerligt och ohanterligt. Oproportionerligt därför att ett godtyckligt införande av nya skyldigheter för en öppen och icke-definierad kategori såsom alla ”leverantörer av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster” inte bara är obegripligt, det är inte heller vederbörligen motiverat när det gäller skador som en säkerhetsincident kan åstadkomma. Det riskerar också att medföra ytterligare byråkrati för våra industrisektorer, framför allt de små och medelstora företagen. Ohanterligt eftersom allvarliga tvivel uppstår huruvida behöriga myndigheter skulle kunna hantera alla potentiella anmälningar på ett aktivt sätt som skulle uppmuntra en tvåvägsdialog med marknadsaktörerna i syfte att lösa säkerhetshotet.

När det gäller **offentliga myndigheter** bör man i direktivet balansera behovet av ytterligare

utveckling av e-förvaltningstjänster mot de redan befintliga skyldigheterna att visa tillbörlig aktsamhet för offentliga myndigheter när det gäller förvaltning och skydd av deras nät och informationssystem. Föredraganden anser därför att även om kraven på utbyte av information som anges i artikel 14 bör tillämpas fullt ut på offentliga myndigheter bör de inte omfattas av skyldigheten i artikel 15.

Andra principen – tillit

Föredragandens anser att en stor del av direktivets framgångar ligger i dess förmåga att sporra marknadens aktörer att bli delaktiga, vilket leder till inrättandet av tillförlitliga NIS-miljöer där de som befinner sig på fältet är beredda att delta aktivt. Om man inte uppnår det med direktivet, kommer det att misslyckas. I det sammanhanget föreslår föredraganden att man ska garantera att marknadsaktörernas deltagande och anmälan inte negativt ska påverkas av onödiga offentliggöranden av säkerhetsincidenter de har anmält, eller att de kan hållas ansvariga för informationsförluster från behöriga myndigheter eller centrala kontaktpunkter. Dessutom måste en tvåvägsdialog upprättas mellan aktörer och behöriga myndigheter och marknadsaktörernas deltagande måste uppmuntras inom alla forum, inbegripet samarbetsnätverket.

Föredraganden anser också att tillit ska vara stöttepelaren för de behöriga myndigheternas och/eller de centrala kontaktpunkternas deltagande, särskilt vad gäller informationsutbyte. För att säkerställa detta bör bestämmelser rörande sekretess och säkerhetskrav för nätet återspeglas i direktivet.

ÄNDRINGSFÖRSLAG

Utskottet för industrifrågor, forskning och energi uppmanar utskottet för den inre marknaden och konsumentskydd att som ansvarigt utskott infoga följande ändringsförslag i sitt betänkande:

Ändringsförslag 1

Förslag till direktiv
Skäl 1

Kommissionens förslag	*Ändringsförslag*
(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion.	(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ***EU-medborgarnas frihet och övergripande säkerhet samt för*** ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion.

Ändringsförslag 2

Förslag till direktiv
Skäl 2

Kommissionens förslag	*Ändringsförslag*
(2) ***Avsiktliga eller oavsiktliga*** säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.	(2) Säkerhetsincidenter blir allt mer omfattande och vanliga ***och deras inverkan allt kraftigare***, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. ***Dessa system kan också bli ett lätt mål för avsiktligt sabotage som går ut på att skada dem eller avbryta deras funktion.*** Sådana incidenter kan ***hota invånarnas säkerhet och hälsa,*** hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas ***och investerarnas*** förtroende och medföra allvarliga konsekvenser för unionens ekonomi.

Motivering

It-angrepp mot börsnoterade företag är en utbredd företeelse och inkluderar stöld av finansiella tillgångar, immateriella rättigheter och störning av verksamheten för företagens kunder eller affärspartner och kan inverka på relationerna med aktieägarna samt på potentiella investerares beslut.

Ändringsförslag 3

Förslag till direktiv
Skäl 3

Kommissionens förslag	*Ändringsförslag*
(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar	(3) Som ett kommunikationsinstrument utan ***traditionella*** gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster***, idéer*** och personer. Denna transnationella natur innebär att störningar

i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad.	i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad ***och dessutom för fungerande yttre marknader***.

Motivering

Att den inre marknadens nät och informationssystem är motståndskraftiga och stabila är också mycket viktigt för samspelet med globala och regionala marknader såsom Nordamerika eller Asien etc.

Ändringsförslag 4

Förslag till direktiv
Skäl 4

Kommissionens förslag	*Ändringsförslag*
(4) En samarbetsmekanism bör inrättas på unionsnivå för att möjliggöra informationsutbyte och samordning av upptäckt och samordnade svarsåtgärder när det gäller nät- och informationssäkerhet. För att denna mekanism ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå av nät- och informationssäkerhet på det egna territoriet. Minimikrav avseende säkerhet bör också gälla för offentliga ***förvaltningar*** och operatörer av ***kritisk*** informationsinfrastrukturer, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras.	(4) En samarbetsmekanism bör inrättas på unionsnivå för att möjliggöra informationsutbyte och samordning av ***förebyggande åtgärder,*** upptäckt och svarsåtgärder när det gäller nät- och informationssäkerhet. För att denna mekanism ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå av nät- och informationssäkerhet på det egna territoriet. Minimikrav avseende säkerhet bör också gälla för offentliga och ***privata*** operatörer av informationsinfrastruktur ***och börsnoterade företag***, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras. ***Den rättsliga ramen bör baseras på behovet av att skydda medborgarens privatliv och integritet. Nätverket för varningar om hot mot kritisk infrastruktur (Ciwin) bör utvidgas till dessa operatörer.***

Motivering

Säkerhetsöverträdelser riktade mot börsnoterade företag kan i hög grad påverka företagets

produkter, tjänster, relationer med kunder och leverantörer, och konkurrensvillkoren generellt och kan därför ha stora konsekvenser för hur den inre (samt yttre) marknaden fungerar. Därför bör även börsnoterade företag omfattas av detta direktiv.

Ändringsförslag 5

Förslag till direktiv
Skäl 4a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4a) Detta direktiv bör vara inriktat på kritisk infrastruktur som är nödvändig för att upprätthålla viktig ekonomisk och samhällelig verksamhet inom områdena energi, transport, bankverksamhet, finansmarknadsinfrastrukturer samt hälso- och sjukvård.

Ändringsförslag 6

Förslag till direktiv
Skäl 4b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4b) För att inte de styrande ska överskrida eller missbruka sina befogenheter är det av största vikt att offentliga myndigheters informations- och säkerhetssystem är öppna för insyn, berättigade, väldefinierade och antagna i öppen demokratisk ordning.

Ändringsförslag 7

Förslag till direktiv
Skäl 6

Kommissionens förslag	*Ändringsförslag*
(6) Den befintliga kapaciteten räcker inte	(6) Den befintliga kapaciteten räcker inte

för att säkerställa en hög nivå av nät- och informationssäkerhet i unionen. Medlemsstaterna har väldigt olika nivåer av beredskap, vilket leder till fragmenterade angreppssätt i unionen. Resultatet blir olika grad av skydd för konsumenter och företag, vilket undergräver den allmänna nät- och informationssäkerhetsnivån i unionen. Avsaknaden av gemensamma minimikrav för ***offentliga förvaltningar och*** marknadsoperatörer gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå.	för att säkerställa en hög nivå av nät- och informationssäkerhet i unionen. Medlemsstaterna har väldigt olika nivåer av beredskap, vilket leder till fragmenterade angreppssätt i unionen. Resultatet blir olika grad av skydd för konsumenter och företag, vilket undergräver den allmänna nät- och informationssäkerhetsnivån i unionen. Avsaknaden av gemensamma minimikrav för marknadsoperatörer gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå***, vilket dessutom skadar det internationella samarbetets effektivitet och följaktligen kampen mot globala säkerhetsutmaningar och undergräver EU:s ledande ställning internationellt i arbetet med att skydda och främja ett öppet, effektivt och säkert internet***.

Ändringsförslag 8

Förslag till direktiv
Skäl 7

Kommissionens förslag	*Ändringsförslag*
(7) Effektiva reaktioner på utmaningarna på nät- och informationssäkerhetsområdet förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam lägsta nivå för kapacitetsuppbyggnad och planering, utbyte av information och samordning av åtgärder samt gemensamma minimikrav avseende säkerhet ***för alla berörda marknadsoperatörer och offentliga förvaltningar***.	(7) Effektiva reaktioner på utmaningarna på nät- och informationssäkerhetsområdet förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam lägsta nivå för kapacitetsuppbyggnad och planering, ***utveckling av tillräcklig kompetens inom it-säkerhet,*** utbyte av information och samordning av åtgärder samt gemensamma minimikrav avseende säkerhet. ***Gemensamma minimistandarder bör tillämpas i enlighet med relevanta rekommendationer från samordningsgrupper för it-säkerhet (Cyber Security Co-Ordination Groups – CSGC).***

Ändringsförslag 9

Förslag till direktiv
Skäl 9

Kommissionens förslag	*Ändringsförslag*
(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå utarbeta planer för samarbete om nät- och informationssäkerhet med grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter.	(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå***, på grundval av de minimikrav som anges i detta direktiv,*** utarbeta planer för samarbete om nät- och informationssäkerhet med grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter. ***Varje medlemsstat bör därför vara skyldig att följa gemensamma standarder för uppgifters format och utbytbarheten av uppgifter som ska utbytas och utvärderas. Medlemsstaterna kan be om stöd från Europeiska byrån för nät- och informationssäkerhet (Enisa) i utvecklingen av sina nationella strategier för nät- och informationssäkerhet, på grundval av en gemensam grundläggande strategisk plan för nät- och informationssäkerhet.***

Motivering

Enisa erkänns redan av relevanta aktörer som ett mycket kompetent kunskapscentrum och ett tillförlitligt verktyg för att främja it-säkerheten i EU. Därför bör EU undvika dubblering av insatser och strukturer och utgå från Enisas kunnande och kräva att Enisa erbjuder rådgivningstjänster till de medlemsstater som saknar institutioner och expertis inom nät- och informationssäkerhet och som begär denna typ av stöd.

Ändringsförslag 10

Förslag till direktiv
Skäl 10

Kommissionens förslag	*Ändringsförslag*
(10) För att uppnå ett effektivt genomförande av de bestämmelser som antas i enlighet med detta direktiv bör man i varje medlemsstat inrätta eller utse ett organ med ansvar för samordning av nät- och informationssäkerhetsfrågor som kan fungera som sambandspunkt för det gränsöverskridande samarbetet på unionsnivå. Dessa organ bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå detta direktivs mål.	(10) För att uppnå ett effektivt genomförande av de bestämmelser som antas i enlighet med detta direktiv bör man i varje medlemsstat inrätta eller utse ett organ med ansvar för samordning av nät- och informationssäkerhetsfrågor som kan fungera som ***gemensam*** sambandspunkt för ***både den interna samordningen och*** det gränsöverskridande samarbetet på unionsnivå. ***Dessa gemensamma nationella kontaktpunkter bör utses utan att det påverkar varje medlemsstats möjlighet att utse fler än en nationell behörig myndighet med ansvar för nät- och informationssäkerhet, enligt sina konstitutionella, rättsliga eller administrativa krav, men bör inte desto mindre utses med ett samordnande mandat på nationell nivå och unionsnivå.*** Dessa organ bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett ***kontinuerligt och*** effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå detta direktivs mål.

Ändringsförslag 11

Förslag till direktiv
Skäl 10a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(10a) Med tanke på att de nationella förvaltningsstrukturerna skiljer sig åt och för att skydda befintliga sektorssystem och undvika dubblering bör medlemsstaterna kunna utse mer än en nationell myndighet med ansvar för uppgifterna i samband med marknadsoperatörernas

nät- och informationssäkerhet enligt detta direktiv. För att se till att gränsöverskridande samarbete och kommunikation fungerar smidigt är det emellertid nödvändigt att varje medlemsstat utser endast en nationell gemensam kontaktpunkt med ansvar för det gränsöverskridande samarbetet på unionsnivå. Om så krävs enligt den konstitutionella strukturen eller andra system bör en medlemsstat få utse endast en myndighet som utövar både den behöriga myndighetens och den gemensamma kontaktpunktens uppgifter.

Ändringsförslag 12

Förslag till direktiv
Skäl 11

Kommissionens förslag	*Ändringsförslag*
(11) Samtliga medlemsstater bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, reagera på och begränsa effekterna av incidenter och risker vad gäller nät och informationssystem. Välfungerade incidenthanteringsorganisationer som uppfyller grundläggande krav bör därför inrättas i alla medlemsstater för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå.	(11) Samtliga medlemsstater ***och marknadsoperatörer*** bör ha både den tekniska och organisatoriska kapacitet som krävs för att ***vid vilken tidpunkt som helst*** förebygga, upptäcka, reagera på och begränsa effekterna av incidenter och risker vad gäller nät och informationssystem. ***Säkerhetssystem för offentlig förvaltning måste vara säkra och stå under demokratisk kontroll och granskning. Deras gängse nödvändiga utrustning och kapacitet bör följa gemensamt överenskomna tekniska standarder samt operationella standardförfaranden.*** Välfungerade incidenthanteringsorganisationer som uppfyller grundläggande krav bör därför inrättas i alla medlemsstater för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. ***Dessa organisationer bör ges möjlighet till samarbete utgående från gemensamma tekniska standarder samt***

operationella standardförfaranden Eftersom de befintliga incidenthanteringsorganisationerna har olika karaktär och svarar mot olika behov och aktörer, bör medlemsstaterna garantera att åtminstone en incidenthanteringsorganisation tillhandahåller tjänster till var och en av de sektorer som omfattas av bilaga II. Medlemsstaterna bör säkerställa att incidenthanteringsorganisationerna har tillräckliga medel för att delta i gränsöverskridande samarbete i de befintliga internationella och europeiska samarbetsnätverken.

Motivering

Interoperabiliteten måste garanteras.

Ändringsförslag 13

Förslag till direktiv
Skäl 12

Kommissionens förslag	*Ändringsförslag*
(12) På grundval av de betydande framsteg som gjorts inom det europeiska forumet för medlemsstaterna (EFMS) när det gäller att främja diskussioner och utbyten av bästa praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid cyberkriser bör medlemsstaterna och kommissionen bilda ett nätverk som för samman dem för kontinuerlig kommunikation och stöder deras samarbete. En sådan säker och effektiv samarbetsmekanism bör skapa förutsättningar för ett strukturerat och samordnat genomförande av informationsutbyte, upptäckt och svarsåtgärder på unionsnivå.	(12) På grundval av de betydande framsteg som gjorts inom det europeiska forumet för medlemsstaterna (EFMS) när det gäller att främja diskussioner och utbyten av bästa praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid cyberkriser bör medlemsstaterna och kommissionen bilda ett nätverk som för samman dem för kontinuerlig kommunikation och stöder deras samarbete. En sådan säker och effektiv samarbetsmekanism***, där marknadsoperatörernas deltagande garanteras,*** bör skapa förutsättningar för ett strukturerat och samordnat genomförande av informationsutbyte, upptäckt och svarsåtgärder på unionsnivå.

Ändringsförslag 14

Förslag till direktiv
Skäl 13

Kommissionens förslag	*Ändringsförslag*
(13) Europeiska byrån för nät- och informationssäkerhet (Enisa) bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och främja utbyte av bästa praxis. Vid tillämpningen av detta direktiv bör kommissionen i synnerhet konsultera Enisa. För att medlemsstaterna och kommissionen i rätt tid ska få den information som behövs bör tidiga varningar om incidenter och risker lämnas inom samarbetsnätverket. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsnätverket också fungera som ett instrument för utbyte av bästa praxis och bistå sina medlemmar vid kapacitetsuppbyggnad samt leda organiserandet av sakkunnigbedömning och nät- och informationssäkerhetsövningar.	(13) Europeiska byrån för nät- och informationssäkerhet (Enisa) bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och främja utbyte av bästa praxis. Vid tillämpningen av detta direktiv bör kommissionen ***och medlemsstaterna*** i synnerhet konsultera Enisa. För att medlemsstaterna och kommissionen i rätt tid ska få den information som behövs bör tidiga varningar om incidenter och risker lämnas inom samarbetsnätverket. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsnätverket också fungera som ett instrument för utbyte av bästa praxis och bistå sina medlemmar vid kapacitetsuppbyggnad samt leda organiserandet av sakkunnigbedömning och nät- och informationssäkerhetsövningar.

Ändringsförslag 15

Förslag till direktiv
Skäl 14

Kommissionens förslag	*Ändringsförslag*
(14) En säker infrastruktur ***bör*** upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas inom samarbetsnätverket. Utan att det påverkar medlemsstaternas skyldighet att anmäla incidenter och risker med en unionsdimension till samarbetsnätverket bör medlemsstater inte få tillgång till konfidentiell information från andra medlemsstater förrän de kan visa att deras tekniska och finansiella resurser,	(14) ***Under Enisas tillsyn bör*** en säker infrastruktur upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas inom samarbetsnätverket. Utan att det påverkar medlemsstaternas skyldighet att anmäla incidenter och risker med en unionsdimension till samarbetsnätverket bör medlemsstater inte få tillgång till konfidentiell information från andra medlemsstater förrän de kan visa att deras

personalresurser och kommunikationsinfrastruktur garanterar att de kan delta i nätverket på ett effektivt, verkningsfullt och säkert sätt.	tekniska och finansiella resurser, personalresurser och kommunikationsinfrastruktur garanterar att de kan delta i nätverket på ett effektivt, verkningsfullt och säkert sätt. ***För att samarbetsnätverket effektivt ska kunna fullgöra sitt uppdrag, bör kommissionen inrätta en budgetrubrik för nätverket.***

Ändringsförslag 16

Förslag till direktiv
Skäl 14a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(14a) Vid behov får även marknadsoperatörer inbjudas att delta i samarbetsnätverkets verksamhet.

Ändringsförslag 17

Förslag till direktiv
Skäl 15

Kommissionens förslag	*Ändringsförslag*
(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor. Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och utbyta information och bästa praxis i utbyte mot operativt stöd vid incidenter.	(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor. Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och ***sinsemellan*** utbyta information och bästa praxis***, inklusive gemensam sådan,*** i utbyte mot ***relevant*** information och operativt stöd ***och strategiskt analyserad information*** vid incidenter. ***För att effektivt uppmuntra utbyte av information och bästa praxis är det mycket viktigt att se till att marknadsoperatörer som deltar i sådana utbyten inte missgynnas till följd***

	av att de samarbetar. Tillräckliga skyddsmekanismer behövs för att inte sådant samarbete ska utsätta dessa operatörer för högre efterlevnadsrisk eller nya ansvarsskyldigheter enligt bland annat lagstiftningen om konkurrens, immateriella rättigheter, uppgiftsskydd eller it-brottslighet, och inte heller för ökade operativa risker eller säkerhetsrisker.

Ändringsförslag 18

Förslag till direktiv
Skäl 16

Kommissionens förslag	*Ändringsförslag*
(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de ***behöriga myndigheterna*** skapa en gemensam webbplats för offentliggörande av sådan information om incidenter ***och*** risker som inte är konfidentiell.	(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de ***gemensamma kontaktpunkterna*** skapa en gemensam ***EU-omfattande*** webbplats för att offentliggöra sådan information om incidenter***,*** risker ***och riskreduceringssätt*** som inte är konfidentiell ***och för att eventuellt ge råd om lämpliga underhållsåtgärder***.

Ändringsförslag 19

Förslag till direktiv
Skäl 17

Kommissionens förslag	*Ändringsförslag*
(17) När information anses konfidentiell enligt unionens bestämmelser och nationella bestämmelser om företagshemlighet bör denna konfidentialitet säkerställas vid genomförande av verksamheter och uppfyllande av mål enligt detta direktiv.	(17) ***Den policy för klassificering av information som avses i skäl 14 bör följa det av Enisa rekommenderade Information Sharing Traffic Light Protocol. All information som utbyts ska klassificeras och hanteras enligt sin grad av känslighet, sådan den angetts av***

informationskällan. När information anses konfidentiell enligt unionens bestämmelser och nationella bestämmelser om företagshemlighet bör denna konfidentialitet säkerställas vid genomförande av verksamheter och uppfyllande av mål enligt detta direktiv.

Ändringsförslag 20

Förslag till direktiv
Skäl 18

Kommissionens förslag	*Ändringsförslag*
(18) På grundval av i synnerhet de nationella erfarenheterna av krishantering bör kommissionen och medlemsstaterna, i samarbete med Enisa, utarbeta en unionsplan för nät- och informationssäkerhetssamarbete som omfattar samarbetsmekanismer för att bemöta risker och incidenter. Planen bör vederbörligen beaktas när tidiga varningar görs inom samarbetsnätverket.	(18) På grundval av i synnerhet de nationella erfarenheterna av krishantering bör kommissionen och medlemsstaterna, i samarbete med Enisa, utarbeta en unionsplan för nät- och informationssäkerhetssamarbete som omfattar samarbetsmekanismer***, bästa praxis och operationsmönster*** för att ***förebygga, upptäcka, rapportera och*** bemöta risker och incidenter. Planen bör vederbörligen beaktas när tidiga varningar görs inom samarbetsnätverket.

Ändringsförslag 21

Förslag till direktiv
Skäl 19

Kommissionens förslag	*Ändringsförslag*
(19) Anmälan av en tidig varning inom nätverket bör endast krävas när den berörda incidenten eller risken är av sådan omfattning och så allvarlig att den är eller kan bli så betydande att det är nödvändigt med information eller samordning av svarsåtgärderna på unionsnivå. Tidiga varningar bör därför begränsas till ***faktiska eller potentiella*** incidenter eller risker som är av snabbt ökande omfattning, som	(19) Anmälan av en tidig varning inom nätverket bör endast krävas när den berörda incidenten eller risken är av sådan omfattning och så allvarlig att den är eller kan bli så betydande att det är nödvändigt med information eller samordning av svarsåtgärderna på unionsnivå. Tidiga varningar bör därför begränsas till incidenter eller risker som är av snabbt ökande omfattning, som överstiger den

överstiger den nationella beredskapen eller som påverkar mer än en medlemsstat. För att möjliggöra en riktig utvärdering bör all information av relevans för bedömningen av risken eller incidenten meddelas samarbetsnätverket.

nationella beredskapen eller som påverkar mer än en medlemsstat. För att möjliggöra en riktig utvärdering bör all information av relevans för bedömningen av risken eller incidenten meddelas samarbetsnätverket.

Ändringsförslag 22

Förslag till direktiv
Skäl 20

Kommissionens förslag	*Ändringsförslag*
(20) Vid mottagandet av en tidig varning, och vid sin bedömning av den, bör de ***behöriga myndigheterna*** enas om samordnade svarsåtgärder i enlighet med unionens plan för nät- och informationssäkerhetssamarbete. ***Behöriga myndigheter*** bör, liksom kommissionen, informeras om de åtgärder som vidtas på nationell nivå till följd av de samordnade svarsåtgärderna.	(20) Vid mottagandet av en tidig varning, och vid sin bedömning av den, bör de ***gemensamma kontaktpunkterna*** enas om samordnade svarsåtgärder i enlighet med unionens plan för nät- och informationssäkerhetssamarbete. ***De gemensamma kontaktpunkterna och Enisa*** bör, liksom kommissionen, informeras om de åtgärder som vidtas på nationell nivå till följd av de samordnade svarsåtgärderna.

Ändringsförslag 23

Förslag till direktiv
Skäl 22

Kommissionens förslag	*Ändringsförslag*
(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på offentliga förvaltningar och marknadsoperatörer. En kultur av riskhantering, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Lika	(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på offentliga förvaltningar och marknadsoperatörer. En kultur av riskhantering***, nära samarbete och förtroende***, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis.

konkurrensvillkor för alla krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.

Lika konkurrensvillkor ***som gäller*** för alla ***på ett tillförlitligt sätt*** krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.

Ändringsförslag 24

Förslag till direktiv
Skäl 24

Kommissionens förslag	*Ändringsförslag*
(24) Dessa skyldigheter bör utvidgas bortom sektorn för elektronisk kommunikation till viktiga leverantörer av informationssamhällets tjänster, enligt definitionen i Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster[4], som ligger till grund för informationssamhällets tjänster i senare led eller onlineverksamhet, t.ex. e-handelsplattformar, ***internetbelningsslussar***, sociala nät, sökmotorer, molntjänster och onlineförsäljning av tillämpningar. ***Störningar i denna typ av informationssamhällestjänster hindrar tillhandahållandet av andra informationssamhällestjänster som är beroende av dem. Programutvecklare och hårdvarutillverkare är inte leverantörer av informationssamhällets tjänster och omfattas därför inte.*** Dessa ***skyldigheter bör också utvidgas till att omfatta offentliga förvaltningar och operatörer av kritisk infrastruktur som är starkt beroende av informations- och kommunikationsteknik och som behövs för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, börser och hälso- och sjukvård. Störningar i dessa nät och***	(24) Dessa skyldigheter bör också utvidgas bortom sektorn för elektronisk kommunikation till ***att omfatta operatörer av infrastruktur som är starkt beroende av informations- och kommunikationsteknik och som är väsentliga för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, finansmarknadsinfrastrukturer och hälso- och sjukvård. Störningar i dessa nät och informationssystem skulle påverka den inre marknaden. Fastän de skyldigheter som framställs i detta direktiv inte omfattar*** viktiga leverantörer av informationssamhällets tjänster, enligt definitionen i Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster, som ligger till grund för informationssamhällets tjänster i senare led eller onlineverksamhet, t.ex. e-handelsplattformar, ***internetbetalningsslussar***, sociala nät, sökmotorer, molntjänster ***överlag*** och onlineförsäljning av tillämpningar. Dessa ***kan dock, på frivillig basis, informera den behöriga myndigheten eller den gemensamma kontaktpunkten om de incidenter i nätverkssäkerheten som de bedömer lämpligt. Den behöriga myndigheten eller den gemensamma***

informationssystem skulle påverka den inre marknaden.	***kontaktpunkten bör då, om det är möjligt inom rimliga gränser, till de marknadsoperatörer som informerat om incidenten tillhandahålla strategiskt analyserad information som bidrar till att avhjälpa säkerhetshotet***.
[27] EGT L 204, 21.7.1998, s. 37.	[27] EGT L 204, 21.7.1998, s. 37.

Ändringsförslag 25

Förslag till direktiv
Skäl 25

Kommissionens förslag	*Ändringsförslag*
(25) Tekniska och organisatoriska åtgärder som införs för ***offentliga förvaltningar och*** marknadsoperatörer bör inte omfatta krav på att en viss kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.	(25) Tekniska och organisatoriska åtgärder som införs för marknadsoperatörer bör inte omfatta krav på att en viss kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt. ***Däremot bör krav ställas på användning av internationella standarder för it-säkerhet.***

Ändringsförslag 26

Förslag till direktiv
Skäl 28

Kommissionens förslag	*Ändringsförslag*
(28) Behöriga myndigheter bör se till att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna bör allmänhetens intresse av att få information om hot vägas mot eventuella negativ inverkan på ryktet och affärerna för de ***offentliga förvaltningar och*** marknadsoperatörer som rapporterar	(28) Behöriga myndigheter ***och gemensamma kontaktpunkter*** bör se till att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. ***Tidigare okända svaga punkter eller incidenter som rapporterats till behöriga myndigheter bör meddelas tillverkaren och tjänsteleverantören av de IKT-produkter och IKT-tjänster som påverkas.*** Vid offentliggörande av

incidenter. Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar ***släpps***.	incidenter som rapporteras till de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** bör allmänhetens intresse av att få information om hot vägas mot eventuella negativ inverkan på ryktet och affärerna för de marknadsoperatörer som rapporterar incidenter. ***För att värna om förtroende och effektivitet bör incidenter offentliggöras endast efter samråd med dem som rapporterat incidenten och enbart när det är absolut nödvändigt för att uppnå målen för detta direktiv.*** Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter ***och gemensamma kontaktpunkter*** särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar ***tas i bruk, men inte fördröja en anmälan mer än vad som nödvändigtvis krävs***. ***Den allmänna regeln bör vara att gemensamma kontaktpunkter inte bör avslöja personuppgifter om dem som är inblandade i incidenter. Kontaktpunkterna bör endast avslöja personuppgifter om det är nödvändigt och proportionellt för ändamålet.***

Motivering

Om myndigheter är medvetna om svaga punkter hos vissa IKT-produkter eller IKT-tjänster, bör de meddela tillverkarna och tjänsteleverantörerna för att de ska hinna anpassa sina produkter och tjänster.

Ändringsförslag 27

Förslag till direktiv
Skäl 29

Kommissionens förslag	*Ändringsförslag*
(29) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att få fram tillräckligt med	(29) Behöriga myndigheter ***och gemensamma kontaktpunkter*** bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet

information från marknadsoperatörer ***och offentliga förvaltningar*** för att bedöma säkerhetsnivån för nät och informationssystem liksom tillförlitliga och heltäckande data om faktiska incidenter som har inverkat på nätens och informationssystemens drift.	befogenhet att få fram tillräckligt med information från marknadsoperatörer för att bedöma säkerhetsnivån för nät och informationssystem ***och mäta incidenters antal, storlek och omfattning,*** liksom tillförlitliga och heltäckande data om faktiska incidenter som har inverkat på nätens och informationssystemens drift.

Ändringsförslag 28

Förslag till direktiv
Skäl 30

Kommissionens förslag	*Ändringsförslag*
(30) I många fall är det kriminell verksamhet som ligger bakom en incident. Incidenternas kriminella art kan misstänkas även om det inte finns några entydiga bevis från början. I sådana fall bör ett lämpligt samarbete mellan behöriga myndigheter och brottsbekämpande myndigheter ingå i effektiva och omfattande svarsåtgärder på hotet från säkerhetsincidenter. För att främja en säker, trygg och mer motståndskraftig miljö krävs i synnerhet en systematisk rapportering av incidenter som misstänks vara av kriminell art till de brottsbekämpande myndigheterna. Incidenters allvarliga kriminella art bör bedömas i ljuset av EU-lagstiftningen om it-brott.	(30) I många fall är det kriminell verksamhet ***eller cyberkrig*** som ligger bakom en incident. Incidenternas kriminella art kan misstänkas även om det inte finns några entydiga bevis från början. I sådana fall bör ett lämpligt samarbete mellan behöriga myndigheter**,** ***gemensamma kontaktpunkter*** och brottsbekämpande myndigheter ***samt samarbete med EC3 (Europol Cybercrime Center) och Enisa*** ingå i effektiva och omfattande svarsåtgärder på hotet från säkerhetsincidenter. För att främja en säker, trygg och mer motståndskraftig miljö krävs i synnerhet en systematisk rapportering av incidenter som misstänks vara av kriminell art till de brottsbekämpande myndigheterna. Incidenters allvarliga kriminella art bör bedömas i ljuset av EU-lagstiftningen om it-brott.

Ändringsförslag 29

Förslag till direktiv
Skäl 31

Kommissionens förslag	*Ändringsförslag*
(31) Säkerheten för personuppgifter äventyras ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna och dataskyddsmyndigheterna samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsbrott till följd av incidenter. ***Medlemsstaterna ska genomföra*** skyldigheten att anmäla säkerhetsincidenter på ett sätt som minimerar den administrativa bördan om säkerhetsincidenten också är ett personuppgiftsbrott ***i linje med förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[5]. Genom samarbete med de behöriga myndigheterna och dataskyddsmyndigheterna skulle*** Enisa ***kunna*** vara till hjälp genom att utveckla mekanismer ***och modeller*** för informationsutbyte ***så att det inte behövs två anmälningsmallar. Denna*** enda anmälningsmall skulle underlätta rapporteringen av incidenter som hotar säkerheten för personuppgifter och därigenom lätta den administrativa bördan för företag och offentliga förvaltningar.	(31) Säkerheten för personuppgifter äventyras ofta till följd av incidenter. ***Medlemsstater och marknadsoperatörer bör skydda personuppgifter som lagras, behandlas eller överförs mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller ändring, och otillåten eller olaglig lagring, utlämning, spridning eller åtkomst, och garantera genomförandet av en säkerhetsstrategi för behandling av personuppgifter.*** I detta sammanhang bör de behöriga myndigheterna***, de gemensamma kontaktpunkterna*** och dataskyddsmyndigheterna samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsbrott till följd av incidenter. Skyldigheten att anmäla säkerhetsincidenter ***bör fullgöras*** på ett sätt som minimerar den administrativa bördan om säkerhetsincidenten också är ett personuppgiftsbrott ***som det är obligatoriskt att anmäla enligt tillämplig lagstiftning.*** Enisa ***bör*** vara till hjälp genom att utveckla mekanismer för informationsutbyte ***och en*** enda anmälningsmall ***som*** skulle underlätta rapporteringen av incidenter som hotar säkerheten för personuppgifter och därigenom lätta den administrativa bördan för företag och offentliga förvaltningar.

[28] SEK(2012) 72 slutlig.

Motivering

Anpassad till förslaget till dataskyddsdirektiv.

Ändringsförslag 30

Förslag till direktiv
Skäl 32

Kommissionens förslag	*Ändringsförslag*
(32) Standardisering av säkerhetskrav är en marknadsdriven process. För att säkerställa en konvergerad tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade standarder för att garantera en hög säkerhetsnivå på unionsnivå. Därför kan det vara nödvändigt att ***utarbeta*** harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG[6].	(32) Standardisering av säkerhetskrav är en marknadsdriven process ***av frivillig karaktär som bör möjliggöra för marknadsoperatörer att använda alternativa metoder för att uppnå åtminstone liknande resultat***. För att säkerställa en konvergerad tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade ***interoperabla*** standarder för att garantera en hög säkerhetsnivå på unionsnivå. Därför ***behöver tillämpning av öppna internationella standarder för nät- och informationssäkerhet eller utformning av sådana verktyg övervägas. Ett ytterligare framsteg som*** kan vara nödvändigt ***är*** att ***det utarbetas*** harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG29. ***Särskilt bör Etsi, Cen och Cenelec uppdras att föreslå effektiva och ändamålsenliga öppna säkerhetsstandarder för EU, där tekniska preferenser undviks så långt möjligt, och som bör vara lätthanterligt för små och medelstora marknadsoperatörer. Internationella standarder för it-säkerhet bör vara noggrant granskade för att säkra att de inte har kompromitterats och att de ger en tillräcklig säkerhetsnivå, och sålunda garanterar att den föreskrivna efterlevnaden av it-säkerhetsstandarder ökar unionens it-säkerhet som helhet och inte minskar den.***

[5] EUT L 316, 14.11.2012, s. 12.

[5] EUT L 316, 14.11.2012, s. 12.

Ändringsförslag 31

Förslag till direktiv
Skäl 33

Kommissionens förslag	*Ändringsförslag*
(33) Detta direktiv bör ses över ***av kommissionen*** med jämna mellanrum, främst i syfte att avgöra behovet av modifieringar med hänsyn till den tekniska utvecklingen eller ändrade marknadsvillkor.	(33) Detta direktiv bör ses över ***av kommissionen*** med jämna mellanrum, ***i samråd med alla berörda aktörer,*** främst i syfte att avgöra behovet av modifieringar med hänsyn till ***samhällsutvecklingen, den politiska utvecklingen,*** den tekniska utvecklingen eller ändrade marknadsvillkor.

Ändringsförslag 32

Förslag till direktiv
Skäl 34

Kommissionens förslag	*Ändringsförslag*
(34) För att se till att samarbetsnätverket fungerar på ett korrekt sätt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på fastställandet av de kriterier som en medlemsstat ska uppfylla för att ha rätt att delta i det säkra informationsutbytessystemet, ytterligare specificering av de händelser som utlöser tidig varning och definitionen av de omständigheter då marknadsoperatörer och offentliga förvaltningar är skyldiga att anmäla incidenter.	***utgår***

Ändringsförslag 33

Förslag till direktiv
Skäl 35

Kommissionens förslag	*Ändringsförslag*
(35) Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, ***inklusive*** på expertnivå. ***Vid förberedelse och utarbetande av delegerade akter bör*** kommissionen ***säkerställa*** att relevanta ***dokument*** samtidigt***, utan dröjsmål och på lämpligt sätt lämnas*** till Europaparlamentet och rådet.	(35) Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, ***med alla berörda parter och särskilt*** på expertnivå. Kommissionen ***bör se till*** att relevanta ***handlingar*** samtidigt ***översänds*** till Europaparlamentet och rådet ***och att detta sker så snabbt som möjligt och på ett lämpligt sätt***.

Ändringsförslag 34

Förslag till direktiv
Skäl 36

Kommissionens förslag	*Ändringsförslag*
(36) För att säkerställa enhetliga villkor för genomförandet av direktivet bör kommissionen ges genomförandebefogenheter när det gäller samarbetet mellan ***behöriga myndigheter*** och kommissionen inom samarbetsnätverket, ***tillträdet till*** den säkra infrastrukturen för informationsutbyte, unionens samarbetsplan för nät- och informationssäkerhet***,*** formaten och förfarandena för att ***informera allmänheten om*** incidenter ***samt standarderna och/eller de tekniska specifikationerna av betydelse för nät- och informationssäkerhet***. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter30.	(36) För att säkerställa enhetliga villkor för genomförandet av direktivet bör kommissionen ges genomförandebefogenheter när det gäller samarbetet mellan ***gemensamma kontaktpunkter*** och kommissionen inom samarbetsnätverket, ***utan att det påverkar befintliga samarbetsmekanismer på nationell nivå, den gemensamma uppsättningen standarder för samtrafikförmåga och säkerhet för*** den säkra infrastrukturen för informationsutbyte, unionens samarbetsplan för nät- och informationssäkerhet ***och*** formaten och förfarandena för att ***anmäla viktiga*** incidenter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina

	genomförandebefogenheter[7].
[30] EUT L 55, 28.2.2011, s. 13.	[30] EUT L 55, 28.2.2011, s. 13.

Ändringsförslag 35

Förslag till direktiv
Skäl 37

Kommissionens förslag	*Ändringsförslag*
(37) Vid tillämpningen av direktivet bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på EU-nivå, i synnerhet ***inom energi-***, ***transport-*** och hälso- och ***sjukvårdsområdet***.	(37) Vid tillämpningen av direktivet bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på EU-nivå, i synnerhet ***på områdena e-förvaltning, energi***, ***transport*** och hälso- och ***sjukvård***.

Ändringsförslag 36

Förslag till direktiv
Skäl 38

Kommissionens förslag	*Ändringsförslag*
(38) Information som ***den nationella regleringsmyndigheten*** anser vara konfidentiell i enlighet med unionslagstiftning och nationell lagstiftning om affärshemligheter, får endast utbytas med kommissionen ***och*** andra behöriga myndigheter när sådant utbyte är absolut nödvändigt för att tillämpa bestämmelserna i detta direktiv. Den information som utbyts bör begränsas till vad som är relevant och proportionellt för ändamålet med utbytet.	(38) Information som ***en behörig myndighet eller en gemensam kontaktpunkt*** anser vara konfidentiell i enlighet med unionslagstiftning och nationell lagstiftning om affärshemligheter, får endast utbytas med kommissionen***, kommissionens relevanta organ, gemensamma kontaktpunkter och/eller*** andra behöriga ***nationella*** myndigheter när sådant utbyte är absolut nödvändigt för att tillämpa bestämmelserna i detta direktiv. Den information som utbyts bör begränsas till vad som är relevant***, nödvändigt*** och proportionellt för ändamålet med utbytet***, samtidigt som man respekterar på förhand fastställda kriterier för konfidentialitet och säkerhet samt klassifikationsprotokoll, som styr***

förfarandet för informationsutbyte.

Ändringsförslag 37

Förslag till direktiv
Skäl 39

Kommissionens förslag	*Ändringsförslag*
(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse och är därmed berättigad enligt artikel 7 i direktiv 95/46/EG. I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar[8] gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.	(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna ***eller gemensamma kontaktpunkterna*** kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse och är därmed berättigad enligt artikel 7 i direktiv 95/46/EG. I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar[8] gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.
[31] EGT L 145, 31.5.2001, s. 43.	[31] EGT L 145, 31.5.2001, s. 43.

Ändringsförslag 38

Förslag till direktiv
Skäl 41a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(41a) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument har medlemsstaterna åtagit sig att, i de fall detta är berättigat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i ett direktiv och motsvarande delar i nationella instrument för införlivande. När det gäller detta direktiv anser lagstiftaren det vara motiverat att sådana dokument översänds.

Ändringsförslag 39

Förslag till direktiv
Artikel 1 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad och effektiv hantering och samordnade och effektiva svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.	(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad och effektiv hantering och samordnade och effektiva svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem ***med deltagande av relevanta aktörer***.

Ändringsförslag 40

Förslag till direktiv

Artikel 1 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. Informationsutbytet inom samarbetsnätverket enligt kapitel III och anmälan av nät- och informationssäkerhetsincidenter enligt artikel 14 kan förutsätta behandling av personuppgifter. Sådan behandling, som är nödvändig för att tillgodose detta direktivs syfte av allmänintresse ska godkännas av medlemsstaten i enlighet med artikel 7 i direktiv 95/46/EG och direktiv 2002/58/EG, såsom dessa har genomförts i nationell lagstiftning.	6. Informationsutbytet inom samarbetsnätverket enligt kapitel III och anmälan av nät- och informationssäkerhetsincidenter enligt artikel 14 kan förutsätta ***kommunikation med tillförlitliga tredje parter och*** behandling av personuppgifter. Sådan behandling, som är nödvändig för att tillgodose detta direktivs syfte av allmänintresse ska godkännas av medlemsstaten i enlighet med artikel 7 i direktiv 95/46/EG och direktiv 2002/58/EG, såsom dessa har genomförts i nationell lagstiftning. ***Medlemsstaterna ska anta lagstiftningsåtgärder i enlighet med artikel 13 i direktiv 95/46/EG för att offentliga förvaltningar, marknadsoperatörer och behöriga myndigheter inte ska hållas ansvariga för behandling av personuppgifter som är nödvändig för utbyte av information inom samarbetsnätverket och anmälan av incidenter.***

Ändringsförslag 41

Förslag till direktiv
Artikel 2

Kommissionens förslag	*Ändringsförslag*
Medlemsstaterna ska inte vara förhindrade att anta eller behålla bestämmelser som garanterar en högre säkerhetsnivå, utan att det påverkar deras skyldigheter enligt unionslagstiftningen.	Medlemsstaterna ska inte vara förhindrade att anta eller behålla bestämmelser som garanterar en högre säkerhetsnivå ***i enlighet med EU:s stadga om de grundläggande rättigheterna***, utan att det påverkar deras skyldigheter enligt unionslagstiftningen.

Motivering

Medlemsstaternas handlingsfrihet i säkerhetsfrågor måste förutsätta att de respekterar de

rättigheter som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till respekt för privatliv och kommunikationer, rätten till skydd av personuppgifter, näringsfriheten och rätten till ett effektivt rättsmedel.

Ändringsförslag 42

Förslag till direktiv
Artikel 3 – led 1– led b

Kommissionens förslag	*Ändringsförslag*
(b) apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av ***datorbehandlade*** uppgifter, samt	(b) apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av ***digitala*** uppgifter, samt

Ändringsförslag 43

Förslag till direktiv
Artikel 3 – led 1 – led c

Kommissionens förslag	*Ändringsförslag*
(c) ***datorbehandlade*** uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av element som omfattas av ***led*** a och b för att de skall kunna drivas, användas, skyddas och underhållas.	(c) ***digitala*** uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av element som omfattas av ***leden*** a och b för att de skall kunna drivas, användas, skyddas och underhållas. säkerhet:

Ändringsförslag 44

Förslag till direktiv
Artikel 3 – led 2

Kommissionens förslag	*Ändringsförslag*
(2) säkerhet: förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar	(2) säkerhet: förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar

tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem.	tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem. ***”Säkerhet” som det definieras här inkluderar passande teknisk utrustning, lösningar och operativa förfaranden som garanterar de säkerhetskrav som framställs i detta direktiv.***

Ändringsförslag 45

Förslag till direktiv
Artikel 3 – led 4

Kommissionens förslag	*Ändringsförslag*
(4) incident: en omständighet eller händelse som har en faktisk negativ inverkan på säkerheten.	(4) incident: en omständighet eller händelse som ***på rimligt sätt kan identifieras och som*** har en faktisk negativ inverkan på säkerheten.

Motivering

Den ursprungliga formuleringen var för bred och skulle ha försvårat tillämpningen av definitionen.

Ändringsförslag 46

Förslag till direktiv
Artikel 3 – led 5

Kommissionens förslag	*Ändringsförslag*
(5) informationssamhällestjänst: tjänst enligt artikel 1.2 i direktiv 98/34/EG.	***utgår***

Ändringsförslag 47

Förslag till direktiv
Artikel 3 – led 8 – led a

Kommissionens förslag	*Ändringsförslag*
(a) Leverantör av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster; en ej uttömmande förteckning över sådana tjänster finns i bilaga II.	***utgår***

Ändringsförslag 48

Förslag till direktiv
Artikel 3 – led 7

Kommissionens förslag	*Ändringsförslag*
(7) incidenthantering: alla förfaranden som ***stödjer*** analys och begränsning av effekterna av en incident samt svarsåtgärder.	(7) incidenthantering: alla förfaranden som ***stöder upptäckt, förebyggande,*** analys och begränsning av effekterna av en incident samt svarsåtgärder.

Ändringsförslag 49

Förslag till direktiv
Artikel 3 – led 8

Kommissionens förslag	*Ändringsförslag*
(a) Leverantör av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster; en ej uttömmande förteckning över sådana tjänster finns i bilaga II.	

(b) Operatör av ***kritisk*** infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena ***energi-, transport-, bank-, börs-*** samt hälso- och sjukvårdsverksamhet; en ***ej uttömmande*** förteckning över sådana verksamheter finns i bilaga II.	(b) ***Offentlig eller privat*** operatör av infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena ***energi, transport, bankverksamhet, finansmarknader*** samt hälso- och sjukvårdsverksamhet***, där det skulle få betydande konsekvenser i en medlemsstat om infrastrukturen stördes eller förstördes så att dessa funktioner inte längre kan upprätthållas***; en förteckning över sådana verksamheter finns i bilaga II.

Ändringsförslag 50

Förslag till direktiv
Artikel 3 – led 8a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(8a) incident som har en betydande inverkan: en incident som påverkar säkerheten och kontinuiteten för ett informationsnät eller informationssystem och avsevärt stör centrala ekonomiska eller samhälleliga funktioner.

Ändringsförslag 51

Förslag till direktiv
Artikel 3 – led 8b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(8b) (8b) tjänst: den tjänst som tillhandahålls av en marknadsoperatör, med uteslutande av alla andra tjänster från samma enhet.

Ändringsförslag 52

Förslag till direktiv
Artikel 3 – led 11a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11a) reglerad marknad: reglerad marknad enligt definitionen i artikel 4.14 i Europaparlamentets och rådets direktiv 2004/39/EG[11a].
	[11a] Europaparlamentets och rådets direktiv 2004/39/EG av den 21 april 2004 om marknader för finansiella instrument (EUT L 45, 16.2.2005, s. 18).

Ändringsförslag 53

Förslag till direktiv
Artikel 3 – led 11b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11b) multilateral handelsplattform (MTF-plattform): multilateral handelsplattform enligt definitionen i artikel 4.15 i direktiv 2004/39/EG.

Ändringsförslag 54

Förslag till direktiv
Artikel 3 – led 11c (nytt)

Kommissionens förslag	*Ändringsförslag*
	organiserad handelsplattform: ett multilateralt system eller en multilateral facilitet, som inte är en reglerad marknad, en multilateral handelsplattform eller en central motpart, som drivs av ett värdepappersföretag eller en marknadsoperatör, inom vilket flera tredje parters köp- och säljintressen i obligationer, strukturerade finansiella

	produkter, utsläppsrätter eller derivat kan interagera inom systemet så att detta leder till ett avtal i enlighet med bestämmelserna i avdelning II i direktiv 2004/39/EG.

Ändringsförslag 55

Förslag till direktiv
Artikel 4

Kommissionens förslag	*Ändringsförslag*
Medlemsstaterna ska säkerställa en hög säkerhetsnivå för nät och informationssystem på deras territorium i enlighet med detta direktiv.	Medlemsstaterna ska ***fortlöpande*** säkerställa en ***varaktigt*** hög säkerhetsnivå för nät och informationssystem på sitt territorium i enlighet med ***Europeiska unionens stadga om de grundläggande rättigheterna*** och detta direktiv.

Motivering

Medlemsstaternas handlingsfrihet i säkerhetsfrågor måste förutsätta att de respekterar de rättigheter som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till respekt för privatliv och kommunikationer, rätten till skydd av personuppgifter, näringsfriheten och rätten till ett effektivt rättsmedel.

Ändringsförslag 56

Förslag till direktiv
Artikel 5 – punkt 1 – led ea (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ea) Medlemsstaterna får be om stöd från Europeiska byrån för nät- och informationssäkerhet (Enisa) i utvecklingen av sina nationella strategier och nationella samarbetsplaner för nät- och informationssäkerhet, på grundval av en gemensam grundläggande plan för strategi och samarbete i fråga om nät- och informationssäkerhet.

Ändringsförslag 57

Förslag till direktiv
Artikel 5 – punkt 2 – led a

Kommissionens förslag	*Ändringsförslag*
(a) En ***riskbedömningsplan för*** kartläggning av risker ***och*** bedömning av verkningarna av potentiella incidenter.	(a) En ***riskhanteringsram med*** kartläggning***, rangordning, utvärdering och behandling*** av risker**,** bedömning av verkningarna av potentiella incidenter**,** ***handlingsalternativ för förebyggande och kontroll samt kriterier för valet av möjliga motåtgärder***.

Ändringsförslag 58

Förslag till direktiv
Artikel 5 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Definition av roller och ansvarsområden för olika aktörer som deltar i genomförandet av ***planen***.	(b) Definition av roller och ansvarsområden för olika ***myndigheter och övriga*** aktörer som deltar i genomförandet av ***ramen***.

Ändringsförslag 59

Förslag till direktiv
Artikel 6 – rubriken

Kommissionens förslag	*Ändringsförslag*
Nationell behörig myndighet för säkerheten i nät och informationssystem	***Nationella behöriga myndigheter och gemensamma kontaktpunkter*** för säkerheten i nät och informationssystem

Ändringsförslag 60

Förslag till direktiv
Artikel 6 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska utse en ***behörig nationell myndighet*** för säkerheten i nät och informationssystem (*den behöriga myndigheten*).	1. Varje medlemsstat ska utse en ***eller flera nationella behöriga myndigheter*** för säkerheten i nät och informationssystem (***nedan kallad*** *den behöriga myndigheten*).

Ändringsförslag 61

Förslag till direktiv
Artikel 6 – punkt 2a (ny)

Kommissionens förslag	*Ändringsförslag*
	2a. Om en medlemsstat utser fler än en behörig myndighet ska den utse en nationell myndighet, t.ex. en behörig myndighet, till nationell gemensam kontaktpunkt för säkerheten i nät och informationssystem (nedan kallad gemensam kontaktpunkt). Om en medlemsstat utser en enda behörig myndighet, ska den behöriga myndigheten också fungera som gemensam kontaktpunkt.

Ändringsförslag 62

Förslag till direktiv
Artikel 6 – punkt 2b (ny)

Kommissionens förslag	*Ändringsförslag*
	2b. Samma medlemsstats behöriga myndigheter och gemensamma kontaktpunkt ska nära samarbeta kring skyldigheterna enligt detta direktiv.

Ändringsförslag 63

Förslag till direktiv
Artikel 6 – punkt 2c (ny)

Kommissionens förslag	*Ändringsförslag*
	2c. Den gemensamma kontaktpunkten ska tillförsäkra gränsöverskridande samarbete med andra gemensamma kontaktpunkter.

Ändringsförslag 64

Förslag till direktiv
Artikel 6 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Medlemsstaterna ska se till att de behöriga myndigheterna har tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå detta direktivs syften. Medlemsstaterna ska se till att de ***behöriga myndigheterna*** samarbetar på ett effektivt och säkert sätt via det nätverk som avses i artikel 8.	3. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå detta direktivs syften. Medlemsstaterna ska se till att de ***gemensamma kontaktpunkterna*** samarbetar på ett effektivt och säkert sätt via det nätverk som avses i artikel 8.

Ändringsförslag 65

Förslag till direktiv
Artikel 6 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. Medlemsstaterna ska se till att de behöriga myndigheterna får de anmälningar av incidenter som görs av ***offentliga förvaltningar och*** marknadsoperatörer såsom anges i artikel 14.2 och att de tilldelas de genomförande- och verkställighetsbefogenheter som avses i artikel 15.	4. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** får de anmälningar av incidenter som görs av marknadsoperatörer såsom anges i artikel 14.2 och att de tilldelas de genomförande- och verkställighetsbefogenheter som avses i artikel 15.

Ändringsförslag 66

Förslag till direktiv
Artikel 6 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. De behöriga myndigheterna ska ***när så är lämpligt*** samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna ***och dataskyddsmyndigheterna***.	5. De behöriga myndigheterna ska ***å ämbetets vägnar*** samråda ***med dataskyddsmyndigheterna*** och***, när så är lämpligt,*** samarbeta med de relevanta nationella rättsvårdande myndigheterna.

Motivering

Om en enda behörig myndighet utövar tillsyn på nationell nivå, utan samarbete med något annat organ som motvikt, rubbas balansen mellan säkerhet och frihet.

Ändringsförslag 67

Förslag till direktiv
Artikel 6 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. De behöriga myndigheterna ska när så är lämpligt samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.	5. De behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ska när så är lämpligt samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.

Ändringsförslag 68

Förslag till direktiv
Artikel 6 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. Varje medlemsstat ska utan dröjsmål meddela kommissionen ***den*** behöriga ***myndighet*** som utses, denna myndighets uppgifter och alla senare ändringar av detta. Varje medlemsstat ska offentliggöra utnämningen av ***den*** behöriga ***myndigheten***.	6. Varje medlemsstat ska utan dröjsmål meddela kommissionen ***de*** behöriga ***myndigheter och den gemensamma kontaktpunkt*** som utses, denna myndighets uppgifter och alla senare ändringar av detta. Varje medlemsstat ska offentliggöra utnämningen av ***de*** behöriga ***myndigheterna***.

Ändringsförslag 69

Förslag till direktiv
Artikel 7 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska inrätta en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.	1. Varje medlemsstat ska inrätta ***minst*** en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) ***för var och en av de sektorer*** som ***anges i bilaga II, som*** ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.

Ändringsförslag 70

Förslag till direktiv
Artikel 7 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. ***Incidenthanteringsorganisationen*** ska bedriva sin verksamhet under tillsyn av den behöriga myndigheten, som regelbundet ska bedöma om resurserna är tillräckliga, om ***mandatet*** är ***ändamålsenligt*** och om incidenthanteringsförfarandet är effektivt.	5. ***Incidenthanteringsorganisationerna*** ska bedriva sin verksamhet under tillsyn av den behöriga myndigheten ***eller den gemensamma kontaktpunkten***, som regelbundet ska bedöma om resurserna är tillräckliga, om ***mandaten*** är ***ändamålsenliga*** och om incidenthanteringsförfarandet är effektivt.

Ändringsförslag 71

Förslag till direktiv
Artikel 7 – punkt 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	5a. Medlemsstaterna ska se till att incidenthanteringsorganisationerna har

tillräckliga personalresurser och ekonomiska resurser för att aktivt delta i internationella samarbetsnätverk, särskilt sådana nätverk på EU-nivå.

Ändringsförslag 72

Förslag till direktiv
Artikel 7 – punkt 5 – led 1 (nytt)

Kommissionens förslag	*Ändringsförslag*
	(1) Incidenthanteringsorganisationerna ska ges möjlighet och uppmuntras att inleda och delta i gemensamma övningar med andra incidenthanteringsorganisationer, med alla incidenthanteringsorganisationer i medlemsstaterna och med lämpliga institutioner i icke-medlemsstater samt med incidenthanteringsorganisationer inom multinationella och internationella institutioner såsom Nato och FN.

Ändringsförslag 73

Förslag till direktiv
Artikel 7 – punkt 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	5a. Medlemsstaterna får be om stöd från Europeiska byrån för nät- och informationssäkerhet (Enisa) eller från andra medlemsstater i utvecklingen av sina nationella incidenthanteringsorganisationer.

Ändringsförslag 74

Förslag till direktiv
Artikel 8

Kommissionens förslag	*Ändringsförslag*
1. De ***behöriga myndigheterna*** och kommissionen ska bilda ett nätverk (samarbetsnätverk) ***för att*** samarbeta om risker och incidenter som påverkar nät och informationssystem.	1. De ***gemensamma kontaktpunkterna, Europeiska byrån för nät- och informationssäkerhet (Enisa)*** och kommissionen ska bilda ett nätverk (samarbetsnätverk) ***där de ska*** samarbeta om risker och incidenter som påverkar nät och informationssystem.
2. Samarbetsnätverket ska föra samman kommissionen och de ***behöriga myndigheterna*** i kontinuerlig kommunikation. ***På begäran ska*** Europeiska byrån för nät- och informationssäkerhet (Enisa) bistå samarbetsnätverket med expertis och råd.	2. Samarbetsnätverket ska föra samman kommissionen och de ***gemensamma kontaktpunkterna*** i kontinuerlig kommunikation. Europeiska byrån för nät- och informationssäkerhet (Enisa) ***ska*** bistå samarbetsnätverket med expertis och råd. ***Samarbetsnätverket ska, när så är lämpligt, samarbeta med dataskyddsmyndigheterna.***
3. Inom samarbetsnätverket ska de ***behöriga myndigheterna*** göra följande:	3. Inom samarbetsnätverket ska de ***gemensamma kontaktpunkterna*** göra följande:
(a) Sprida tidiga varningar om risker och incidenter i enlighet med artikel 10.	(a) Sprida tidiga varningar om risker och incidenter i enlighet med artikel 10.
(b) Säkerställa samordnade svarsåtgärder i enlighet med artikel 11.	(b) Säkerställa samordnade svarsåtgärder i enlighet med artikel 11.
(c) Regelbundet offentliggöra ej konfidentiell information om pågående tidiga varningar och samordnade svarsåtgärder på en gemensam webbplats.	(c) Regelbundet offentliggöra ej konfidentiell information om pågående tidiga varningar och samordnade svarsåtgärder på en gemensam webbplats.
	(ca) Gemensamt diskutera, komma överens om gemensam tolkning, konsekvent tillämpning och samordna sina åtgärder i fråga om de säkerhetskrav och den anmälan av incidenter som avses i artikel 14 och i fråga om genomförande och efterlevnad enligt artikel 15.
(d) ***På en begäran av en medlemsstat eller kommissionen*** gemensamt diskutera och bedöma en eller leda nationella NIS-strategier och nationella NIS-	(d) Gemensamt diskutera och bedöma en eller leda nationella NIS-strategier och nationella NIS-samarbetsplaner enligt artikel 5, inom detta direktivs räckvidd.

samarbetsplaner enligt artikel 5, inom detta direktivs räckvidd.

(e) På begäran av en medlemsstat eller kommissionen gemensamt diskutera och bedöma incidenthanteringsorganisationernas effektivitet, i synnerhet när NIS-övningar genomförs på unionsnivå.

(e) På begäran av ***Enisa,*** en medlemsstat eller kommissionen gemensamt diskutera och bedöma incidenthanteringsorganisationernas effektivitet, i synnerhet när NIS-övningar genomförs på unionsnivå***, och genomföra åtgärder för att lösa identifierade svagheter utan onödigt dröjsmål***.

(f) Samarbeta och utbyta information om alla relevanta frågor med ***Europeiska it-brottscentrumet inom Europol och med*** andra relevanta europeiska organ, i synnerhet inom områdena ***dataskydd,*** energi, transport, bankverksamhet, ***börs*** och hälso- och sjukvård.

(f) Samarbeta och utbyta information om alla relevanta frågor ***om nät- och informationssäkerhet*** med andra relevanta europeiska organ, i synnerhet inom områdena energi, transport, bankverksamhet, ***finansmarknader*** och hälso- och sjukvård.

(fa) Gemensamt diskutera och komma överens om gemensam tolkning, konsekvent tillämpning och samordnat genomförande inom unionen av bestämmelserna i kapitel IV.

(g) Utbyta information och bästa praxis med varandra och med kommissionen och bistå varandra i uppbyggnaden av NIS-kapacitet.

(g) Utbyta information och bästa praxis med varandra och med kommissionen och bistå varandra i uppbyggnaden av NIS-kapacitet.

(h) Anordna regelbundna kollegiala granskningar av kapacitet och beredskap.

(h) Anordna regelbundna kollegiala granskningar av kapacitet och beredskap.

(i) Anordna NIS-övningar på unionsnivå och delta, såsom lämpligt, i internationella NIS-övningar.

(i) Anordna NIS-övningar på unionsnivå och delta, såsom lämpligt, i internationella NIS-övningar.

(ia) Aktivt främja att marknadsaktörer engageras, rådfrågas och att information utbyts med dessa.

Kommissionen ska regelbundet informera samarbetsnätverket om säkerhetsforskning och andra relevanta program inom Horisont 2020.

3a. Vid behov ska även relevanta offentliga myndigheter och marknadsoperatörer inbjudas att delta i samarbetsnätverkets verksamhet av det slag som avses i punkt 3 c, g, h och i.

	3b. Där information, tidiga varningar eller bästa praxis som kommer från marknadsoperatörer eller offentliga förvaltningar utbyts inom, eller lämnas ut av, samarbetsnätverket ska sådant utbyte eller sådan utlämning ske i enlighet med informationens klassificering såsom den anges av den ursprungliga källan i enlighet med artikel 9.1.
	3c. Kommissionen ska offentliggöra en årlig rapport som grundar sig på nätverkets verksamhet under de senaste tolv månaderna och på den sammanfattande rapport som ska lämnas in i enlighet med artikel 14.4 i detta direktiv. Vid offentliggörande av enskilda incidenter som rapporteras till de behöriga myndigheterna och de gemensamma kontaktpunkterna bör allmänhetens intresse av att få information om hot vägas mot eventuell negativ inverkan på ryktet och affärerna för de marknadsoperatörer som rapporterar incidenter och sådana offentliggöranden får endast ske om de föregåtts av samråd.
4. Kommissionen ska genom genomförandeakter anta de bestämmelser som är nödvändiga för att underlätta samarbetet mellan ***behöriga myndigheter*** och kommissionen enligt punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det samrådsförfarande som avses i artikel 19.2.	4. Kommissionen ska genom genomförandeakter anta de bestämmelser som är nödvändiga för att underlätta samarbetet mellan ***gemensamma kontaktpunkter, Enisa*** och kommissionen enligt punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det samrådsförfarande som avses i artikel 19.2.

Ändringsförslag 75

Förslag till direktiv
Artikel 9 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Känslig och konfidentiell information inom samarbetsnätverket ska utbytas via en	1. Känslig och konfidentiell information inom samarbetsnätverket ska utbytas via en

säker infrastruktur.	säker infrastruktur ***som drivs under tillsyn av Enisa***. ***Medlemsstaterna ska garantera att känslig eller konfidentiell information som överlämnats av andra stater eller kommissionen inte utbyts med tredjeländer eller används för annat ändamål än det avsedda, exempelvis för underrättelsetjänsters verksamhet eller för ekonomiska beslut.***

Ändringsförslag 76

Förslag till direktiv
Artikel 9 – punkt 2 – inledningen

Kommissionens förslag	*Ändringsförslag*
2. Kommissionen ska ha befogenhet att anta ***delegerade akter*** i enlighet med artikel ***18*** när det gäller definitionen av de kriterier som en ***medlemsstat*** ska uppfylla för att godkännas för deltagande i det säkra systemet för informationsutbyte, vad gäller följande:	2. Kommissionen ska ha befogenhet att anta ***genomförandeakter*** i enlighet med artikel ***19*** när det gäller definitionen av de kriterier som en ***gemensam kontaktpunkt*** ska uppfylla för att godkännas för deltagande i det säkra systemet för informationsutbyte, vad gäller följande:

Ändringsförslag 77

Förslag till direktiv
Artikel 9 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Kommissionen ska genom genomförandeakter ***besluta om medlemsstaternas tillträde till denna säkra infrastruktur, i enlighet med de kriterier som avses i punkterna 2 och 3***. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.	3. Kommissionen ska genom genomförandeakter ***anta en gemensam uppsättning standarder för samtrafik och säkerhet som gemensamma kontaktpunkter måste följa för att kunna utbyta information***. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

Ändringsförslag 78

Förslag till direktiv
Artikel 10

Kommissionens förslag	*Ändringsförslag*
1. De ***behöriga myndigheterna*** eller kommissionen ska lämna tidiga varningar inom samarbetsnätverket om de risker eller incidenter som uppfyller minst ett av följande villkor:	1. De ***gemensamma kontaktpunkterna*** eller kommissionen ska lämna tidiga varningar inom samarbetsnätverket om de risker eller incidenter som uppfyller minst ett av följande villkor:
(a) De ökar snabbt i omfattning eller kan öka snabbt i omfattning.	
(b) ***De*** överstiger ***eller kan överstiga*** den nationella kapaciteten för svarsåtgärder.	(b) ***Den gemensamma kontaktpunkten bedömer att risken eller incidenten ökar snabbt i omfattning eller kan öka snabbt i omfattning och potentiellt*** överstiger den nationella kapaciteten för svarsåtgärder.
(c) ***De*** påverkar ***eller kan påverka*** mer än en medlemsstat.	(c) ***De gemensamma kontaktpunkterna eller kommissionen bedömer att risken eller incidenterna*** påverkar mer än en medlemsstat.
2. I de tidiga varningarna ska de ***behöriga myndigheterna*** eller kommissionen meddela all relevant information som de förfogar över och som kan vara till nytta för att bedöma risken eller incidenten.	2. I de tidiga varningarna ska de ***gemensamma kontaktpunkterna*** eller kommissionen ***utan onödigt dröjsmål*** meddela all relevant information som de förfogar över och som kan vara till nytta för att bedöma risken eller incidenten. ***Information som betecknas som hemligstämplad eller konfidentiell av den berörda marknadsoperatören, inklusive marknadsoperatörens identitet, ska tillhandahållas i den utsträckning det är nödvändigt för att bedöma risken eller incidenten.***
3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att en medlemsstat inkommer med relevant information om en specifik risk eller incident.	3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att en medlemsstat inkommer med relevant ***icke-hemligstämplad*** information om en specifik risk eller incident.
4. Om den risk eller incident som är föremål för en tidig varning misstänks vara av brottslig art ska de ***behöriga myndigheterna*** eller kommissionen	4. Om den risk eller incident som är föremål för en tidig varning misstänks vara av ***allvarlig*** brottslig art ska de ***gemensamma kontaktpunkterna*** eller

underrätta Europeiska it-brottscentrumet inom Europol.	kommissionen***, när så är lämpligt, kontakta nationella myndigheter med ansvar för it-brottslighet för att de utan onödigt dröjsmål ska kunna samarbeta och utbyta information med*** Europeiska it-brottscentrumet inom Europol.
	4 a. Medlemmarna i samarbetsnätverket ska inte offentliggöra någon information som mottagits om risker och incidenter enligt punkt 1 utan att ha fått förhandsgodkännande från den gemensamma kontaktpunkt som gjort anmälan.
	4b. Om den risk eller incident som är föremål för en tidig varning misstänks vara av allvarlig gränsöverskridande teknisk art ska de gemensamma kontaktpunkterna eller kommissionen underrätta Enisa.
5. Kommissionen ska ha befogenhet att anta ***delegerade akter*** i enlighet med artikel ***18*** när det gäller ytterligare specificering av risker och incidenter som utlöser en tidig varning enligt punkt 1.	5. Kommissionen ska ha befogenhet att anta ***genomförandeakter*** i enlighet med artikel ***19*** när det gäller ytterligare specificering av risker och incidenter som utlöser en tidig varning enligt punkt 1***, samt om förfaranden för utbyte av information som är känslig för marknadsoperatörer***.

Ändringsförslag 79

Förslag till direktiv
Artikel 11 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Efter en tidig varning enligt artikel 10 ska de ***behöriga myndigheterna***, efter att gjort en bedömning av den relevanta informationen enas om samordnade svarsåtgärder i enlighet med unionens NIS-samarbetsplan enligt artikel 12.	1. Efter en tidig varning enligt artikel 10 ska de ***gemensamma kontaktpunkterna***, efter att gjort en bedömning av den relevanta informationen***, utan onödigt dröjsmål*** enas om samordnade svarsåtgärder i enlighet med unionens NIS-samarbetsplan enligt artikel 12.

Ändringsförslag 80

Förslag till direktiv
Artikel 12 – punkt 2 – led a – strecksats 1

Kommissionens förslag	*Ändringsförslag*
– En definition av format och förfaranden för de ***behöriga myndigheternas*** insamling och utbyte av kompatibla och jämförbara uppgifter om risker och incidenter.	– En definition av format och förfaranden för de ***gemensamma kontaktpunkternas*** insamling och utbyte av kompatibla och jämförbara uppgifter om risker och incidenter.

Ändringsförslag 81

Förslag till direktiv
Artikel 12 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Unionens NIS-samarbetsplan ska antas senast ett år efter detta direktivs ikraftträdande och regelbundet revideras.	3. Unionens NIS-samarbetsplan ska antas senast ett år efter detta direktivs ikraftträdande och regelbundet revideras. ***Resultaten av varje revidering ska rapporteras till Europaparlamentet.***

Ändringsförslag 82

Förslag till direktiv
Artikel 12 – punkt 3a (ny)

Kommissionens förslag	*Ändringsförslag*
	3a. Kommissionen ska tillhandahålla en budget för utvecklingen av unionens NIS-samarbetsplan.

Ändringsförslag 83

Förslag till direktiv
Artikel 13

Kommissionens förslag	*Ändringsförslag*
Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. ***Sådana avtal*** ska ***beakta behovet av ändamålsenligt*** skydd för personuppgifter som förmedlas via samarbetsnätverket.	Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. ***I avtalen*** ska ***det framgå vilket kontrollförfarande som ska tillämpas för att garantera*** skydd för personuppgifter som förmedlas via samarbetsnätverket. ***Europaparlamentet ska informeras om avtalsförhandlingen och få insyn i innehållet. Om personuppgifter överförs till mottagare i länder utanför unionen ska det ske i enlighet med artiklarna 25 och 26 i direktiv 95/46/EG och artikel 9 i förordning (EG) nr 45/2001.***

Motivering

Internationella avtal som ingås med andra länder eller säkerhetsorgan måste innehålla en mekanism för kontroll av respekten för de medborgerliga rättigheterna. Europaparlamentet måste dessutom utöva effektiv demokratisk tillsyn över avtalen och parlamentet ska informeras i god tid om innehållet i avtalsförhandlingarna.

Ändringsförslag 84

Förslag till direktiv
Artikel 14

Kommissionens förslag	*Ändringsförslag*

1. Medlemsstaterna ska se till att ***offentliga förvaltningar och*** marknadsoperatörer vidtar ändamålsenliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten för de nät och informationssystem som de kontroller och använder i sin verksamhet. Med beaktande av den ***senaste tekniken*** ska dessa åtgärder garantera en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga ***och minimera de effekter som*** incidenter som påverkar deras nät och informationssystem ***har*** på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem.

2. Medlemsstaterna ska säkerställa att ***offentliga förvaltningar och*** marknadsoperatörer underrättar den behöriga myndigheten om incidenter som ***har en betydande inverkan på*** säkerheten ***för*** de kärntjänster som de tillhandahåller.

1. Medlemsstaterna ska se till att marknadsoperatörer vidtar ändamålsenliga tekniska och organisatoriska åtgärder för att ***upptäcka och effektivt*** hantera risker som hotar säkerheten för de nät och informationssystem som de kontrollerar och använder i sin verksamhet. Med beaktande av den ***tekniska utvecklingen*** ska dessa ***ändamålsenliga*** åtgärder garantera en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga incidenter som påverkar ***säkerheten hos*** deras nät och informationssystem ***och minimera deras effekter*** på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem.

2. Medlemsstaterna ska ***genomföra mekanismer för att*** säkerställa att marknadsoperatörer ***utan onödigt dröjsmål*** underrättar den behöriga myndigheten ***eller den gemensamma kontaktpunkten*** om incidenter som ***påverkar*** säkerheten ***eller kontinuiteten hos*** de kärntjänster som de tillhandahåller. ***Anmälan ska inte utsätta den anmälande parten för ökad ansvarsskyldighet. För att avgöra hur betydande inverkan en incident har ska man ta hänsyn till bl.a. följande faktorer:***

(a) Hur många användares kärntjänster som påverkas.

(b) Hur länge incidenten varat.

(c) Hur stort geografiskt område som påverkats av incidenten.

Dessa kriterier ska specificeras ytterligare i enlighet med artikel 8.3 ca (ny).

2a. Enheter som inte omfattas av bilaga II får på frivillig väg rapportera incidenter av det slag som anges i artikel 14.2.

2b. Mottagaren av en rapport om en incident ska så snart som möjligt underrätta den enhet som rapporterat incidenten om vilka åtgärder som vidtagits, vilka beslut som fattats eller

vilka rekommendationer som utfärdats, liksom också om eventuella tredje parter som informerats samt om de protokoll om säkerhet och konfidentialitet som styr informationsutbytet.

3. Dessa krav enligt punkterna 1 och 2 gäller för alla marknadsoperatörer som tillhandahåller tjänster inom Europeiska unionen.

3. Dessa krav enligt punkterna 1 och 2 gäller för alla marknadsoperatörer som tillhandahåller tjänster inom Europeiska unionen. ***Marknadsoperatörer som inte tillhandahåller tjänster inom Europeiska unionen får på frivillig väg rapportera incidenter.***

3a. Marknadsoperatörerna ska se till att marknadsoperatörer anmäler de incidenter som avses i punkterna 1 och 2 till den behöriga myndigheten eller den gemensamma kontaktpunkten i den medlemsstat där kärntjänsten påverkas. Om kärntjänster påverkas i fler än en medlemsstat ska den gemensamma kontaktpunkt som har mottagit anmälan meddela övriga berörda gemensamma kontaktpunkter, med utgångspunkt i informationen från marknadsoperatören. Marknadsoperatörer ska så snart som möjligt få veta vilka andra gemensamma kontaktpunkter som underrättats om incidenten, samt om eventuella vidtagna åtgärder, resultat och all annan information av relevans för incidenten.

4. Den behöriga myndigheten ***får*** informera allmänheten ***eller kräva att de offentliga myndigheterna och marknadsoperatörerna informerar allmänheten***, om den fastställer att ***det ligger i allmänhetens intresse att*** incidenten ***röjs***. ***En gång*** om året ska den ***behöriga myndigheten*** lämna in en sammanfattande rapport till samarbetsnätverket om de anmälningar som kommit in och de åtgärder som vidtagits i enlighet med denna punkt.

4. ***Efter samråd med*** den behöriga myndigheten ***och den berörda marknadsoperatören ska den gemensamma kontaktpunkten*** informera allmänheten ***om enskilda incidenter***, om den fastställer att ***allmänheten behöver känna till dessa för att man ska kunna förhindra en incident eller åtgärda en pågående incident, för att medlemmar av allmänheten ska kunna minska risker som rör dem själva och föranleds av incidenten eller om en marknadsoperatör som drabbats av en incident vägrat att utan onödigt dröjsmål åtgärda en allvarlig strukturell sårbarhet i samband med den*** incidenten. ***Den gemensamma kontaktpunkten ska vederbörligen***

motivera beslutet. Den behöriga myndigheten eller den gemensamma kontaktpunkten ska, om det är möjligt inom rimliga gränser, till de marknadsoperatörer som informerat om incidenten tillhandahålla strategiskt analyserad information som bidrar till att avhjälpa säkerhetshotet. Två gånger om året ska den ***gemensamma kontaktpunkten*** lämna in en sammanfattande rapport till samarbetsnätverket om de anmälningar som kommit in och de åtgärder som vidtagits i enlighet med denna punkt. ***Vid offentliggörande av enskilda incidenter som rapporteras till de behöriga myndigheterna och de gemensamma kontaktpunkterna bör allmänhetens intresse av att få information om hot vederbörligen vägas mot eventuell negativ inverkan på ryktet och affärerna för marknadsoperatörer som rapporterar incidenter och sådana offentliggöranden får endast ske om de föregåtts av samråd.***

Vid anmälan av incidenter till det samarbetsnätverk som avses i artikel 8 får andra nationella behöriga myndigheter inte utan godkännande från den anmälande behöriga myndigheten offentliggöra någon information som mottagits om risker eller incidenter.

5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet artikel 18 när det gäller definition av de omständigheter då offentliga förvaltningar och marknadsoperatörer är skyldiga att anmäla incidenter.

6. ***Utan att det påverkar tillämpningen av delegerade akter som antas enligt punkt 5 får*** de behöriga myndigheterna anta riktlinjer ***och, om nödvändigt, utfärda anvisningar*** avseende de omständigheter då ***offentliga förvaltningar och*** marknadsoperatörer är skyldiga att anmäla incidenter.

6. De behöriga myndigheterna ***eller de gemensamma kontaktpunkterna ska*** anta riktlinjer avseende de omständigheter då marknadsoperatörer är skyldiga att anmäla incidenter.

7. Kommissionen ska ha befogenhet att genom genomförandeakter definiera format

7. Kommissionen ska ha befogenhet att genom genomförandeakter definiera format

och förfaranden för tillämpningen av punkt 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

8. Punkterna 1 och 2 ska inte tillämpas på mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag[12].

_____

[12] EGT L 124, 20.5.2003, s. 36.

och förfaranden för tillämpningen av punkt 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

8. Punkterna 1 och 2 ska inte tillämpas på mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag[12].

_____

[12] EGT L 124, 20.5.2003, s. 36.

Ändringsförslag 85

Förslag till direktiv
Artikel 14 – punkt 4 – stycke 1 (nytt)

Kommissionens förslag	*Ändringsförslag*
	Utöver att rapportera till den behöriga myndigheten ska marknadsoperatörer uppmuntras att i sina redovisningar (på frivillig basis) meddela incidenter som involverar deras företag.

Motivering

It-incidenter kan medföra stora finansiella förluster och avsevärda kostnader. Aktieägare och investerare bör informeras om konsekvenserna av dessa incidenter. Genom att uppmuntra företag att offentliggöra it-incidenter på frivillig basis kan man stimulera diskussionen inom olika sektorer om sannolikheten för framtida incidenter, omfattningen av dessa risker, samt lämpligheten av förebyggande åtgärder som vidtas för att minska problem med it-säkerheten.

Ändringsförslag 86

Förslag till direktiv
Artikel 15

Kommissionens förslag	*Ändringsförslag*
1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter de behöver för att ***utreda fall***	1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har de

då offentliga förvaltningar eller marknadsoperatörer inte uppfyllt sina skyldigheter ***enligt*** artikel 14 och de effekter som detta har på nätens och informationssystemens säkerhet.

befogenheter de behöver för att ***säkerställa att de*** skyldigheter ***som följer av*** artikel 14 ***uppfylls, med*** de effekter som detta har på nätens och informationssystemens säkerhet.

2. Medlemsstaterna ska se till att de behöriga myndigheterna har befogenhet att ålägga att marknadsoperatörer ***och offentliga förvaltningar***

2. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har befogenhet att ålägga att marknadsoperatörer

(a) tillhandahåller den information som behövs för en bedömning av säkerheten i deras nät och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och

(a) tillhandahåller den information som behövs för en bedömning av säkerheten i deras nät och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och

(b) ***genomgår*** en säkerhetsrevision som ***utförs*** av ett kvalificerat oberoende organ eller av en nationell myndighet och ***ge*** den behöriga myndigheten tillgång till resultaten.

(b) ***tillhandahåller dokumentation som visar att säkerhetsåtgärderna genomförts effektivt, t.ex. resultaten av*** en säkerhetsrevision som ***utförts*** av ***internrevisorer,*** ett kvalificerat oberoende organ eller av en nationell myndighet och ***ger*** den behöriga myndigheten eller den gemensamma kontaktpunkten tillgång till dokumentationen. ***Vid behov får den behöriga myndigheten eller den gemensamma kontaktpunkten begära ytterligare dokumentation eller i undantagsfall, och med vederbörlig motivering, utföra ytterligare en revision.***

I en sådan begäran ska de behöriga myndigheterna och de gemensamma kontaktpunkterna uppge syftet med begäran och ange tillräckligt tydligt vilken information som begärs.

3. Medlemsstaterna ska se till att de behöriga myndigheterna har befogenhet att utfärda bindande anvisningar för marknadsoperatörer ***och offentliga förvaltningar***.

3. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har befogenhet att utfärda bindande anvisningar för ***alla de*** marknadsoperatörer ***som anges i bilaga II***.

4. De behöriga myndigheterna ska ***anmäla*** incidenter som misstänks vara av allvarlig brottslig art ***till de rättsvårdande myndigheterna***.

4. De behöriga myndigheterna ***och den gemensamma kontaktpunkten*** ska ***informera de berörda marknadsoperatörerna om att de inför de rättsvårdande myndigheterna kan inleda***

	straffrättsliga förfaranden om incidenter som misstänks vara av allvarlig brottslig art.
5. De behöriga myndigheterna ***ska*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott.	5. ***Utan att det påverkar tillämplig dataskyddslagstiftning ska*** de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott. ***De gemensamma kontaktpunkterna och dataskyddsmyndigheterna ska i samarbete med Enisa utforma mekanismer för informationsutbyte och en gemensam mall för anmälningar både enligt artikel 14.2 i detta direktiv och enligt Europaparlamentets och rådets förordning (EU) nr 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.***
	Kommissionen får genom genomförandeakter och med yttersta hänsyn tagen till eventuella mekanismer för informationsutbyte och gemensamma mallar som utformats av de gemensamma kontaktpunkterna och dataskyddsmyndigheterna, i samarbete med Enisa, anta förfaranden för mekanismer för informationsutbyte och den gemensamma mallen.
6. Medlemsstaterna ska säkerställa att alla skyldigheter som införs för ***offentliga förvaltningar och*** marknadsoperatörer i enlighet med detta kapitel kan bli föremål för rättslig prövning.	6. Medlemsstaterna ska säkerställa att alla skyldigheter som införs för marknadsoperatörer i enlighet med detta kapitel kan bli föremål för rättslig prövning.

Ändringsförslag 87

Förslag till direktiv
Artikel 16

Kommissionens förslag	*Ändringsförslag*
1. För att säkerställa en enhetlig	1. För att säkerställa en enhetlig

tillämpning av artikel 14.1 ska medlemsstaterna främja användningen av standarder och/eller specifikationer av relevans för nät- och informationssäkerheten.	tillämpning av artikel 14.1 ska medlemsstaterna***, utan att föreskriva användning av någon särskild teknik,*** främja användningen av ***öppna och interoperabla EU-omfattande internationella*** standarder och/eller specifikationer av relevans för nät- och informationssäkerheten***, som följer unionslagstiftningen***.
2. Kommissionen ska ***i genomförandeakter*** utarbeta en lista över de standarder som avses i punkt 1. Listan ska kungöras i Europeiska unionens officiella tidning.	2. Kommissionen ska ***uppdra åt ett relevant europeiskt standardiseringsorgan att under samråd med relevanta aktörer*** utarbeta en lista över de standarder ***och/eller specifikationer*** som avses i punkt 1. Listan ska kungöras i Europeiska unionens officiella tidning.

Ändringsförslag 88

Förslag till direktiv
Artikel 17 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Medlemsstaterna ska föreskriva påföljder för överträdelser av nationella bestämmelser som har utfärdats med tillämpning av detta direktiv och ska vidta de åtgärder som krävs för att se till att dessa påföljder tillämpas. Påföljderna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa bestämmelser till kommissionen senast det datum då direktivet införlivas med nationell lagstiftning och skall utan dröjsmål anmäla alla senare ändringar som påverkar dem.	1. Medlemsstaterna ska föreskriva påföljder för ***oaktsamma och avsiktliga*** överträdelser av nationella bestämmelser som har utfärdats med tillämpning av detta direktiv och ska vidta de åtgärder som krävs för att se till att dessa påföljder tillämpas. Påföljderna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa bestämmelser till kommissionen senast det datum då direktivet införlivas med nationell lagstiftning och skall utan dröjsmål anmäla alla senare ändringar som påverkar dem.

Motivering

Det bör vara tydligt att påföljder endast kan tillämpas på överträdelser där marknadsoperatörer har underlåtit att vidta alla åtgärder som rimligtvis kunde ha förväntats av dem. Marknadsoperatörer skulle annars kunna avskräckas från att rapportera incidenter.

Ändringsförslag 89

Förslag till direktiv
Artikel 17 – punkt 1a (ny)

Kommissionens förslag	*Ändringsförslag*
	1a. Medlemsstaterna ska se till att de påföljder som avses i punkt 1 i denna artikel är tillämpliga endast om en marknadsoperatör avsiktligt eller till följd av grov oaktsamhet har underlåtit att fullgöra sina skyldigheter enligt kapitel IV.

Ändringsförslag 90

Förslag till direktiv
Artikel 18

Kommissionens förslag	*Ändringsförslag*
Artikel 18	***utgår***
Utövande av delegeringen	
1. Kommissionens rätt att anta delegerade akter gäller på de villkor som fastställs i denna artikel.	
2. Befogenhet att anta de delegerade akter som avses i artiklarna 9.2, 10.5 och 14.5 ska ges till kommissionen. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av femårsperioden. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.	
3. Den delegering av befogenhet som avses i artiklarna 9.2, 10.5 and 14.5 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut	

om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i Europeiska unionens officiella tidning, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. När kommissionen antagit en delegerad akt ska den samtidigt underrätta Europaparlamentet och rådet.

5. En delegerad akt som antas i enlighet med artiklarna 9.2, 10.5 och 14.5 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Ändringsförslag 91

Förslag till direktiv
Artikel 20

Kommissionens förslag	*Ändringsförslag*
Kommissionen ska ***regelbundet*** se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast ***tre*** år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.	Kommissionen ska ***vart tredje år*** se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast ***två*** år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.

Motivering

För att hålla jämna steg med föränderliga hot och villkor på it-säkerhetsområdet ska bilaga II regelbundet ses över och redigeras.

Ändringsförslag 92

Förslag till direktiv
Bilaga I – rubriken

Kommissionens förslag	*Ändringsförslag*
Krav och uppgifter för ***incidenthanteringsorganisationen*** (Cert)	Krav och uppgifter för ***incidenthanteringsorganisationerna*** (Cert)

Ändringsförslag 93

Förslag till direktiv
Bilaga I – inledningen

Kommissionens förslag	*Ändringsförslag*
Incidenthanteringsorganisationens krav och uppgifter ska på lämpligt och entydigt sätt fastställas och stödjas genom nationell politik och/eller lagstiftning. Följande ska ingå:	***Incidenthanteringsorganisationernas*** krav och uppgifter ska på lämpligt och entydigt sätt fastställas och stödjas genom nationell politik och/eller lagstiftning. Följande ska ingå: *(Denna ändring är tillämplig på hela bilaga I.)*

Ändringsförslag 94

Förslag till direktiv
Bilaga I – led 1 – led a

Kommissionens förslag	*Ändringsförslag*
(a) ***Incidenthanteringsorganisationen*** ska säkerställa god tillgång till sina kommunikationstjänster genom att undvika felkritiska systemdelar (single points of failure) och kunna kontaktas och kontakta andra på flera olika sätt. Kommunikationskanalerna ska vara tydligt	(a) ***Incidenthanteringsorganisationerna*** ska säkerställa god tillgång till sina kommunikationstjänster genom att undvika felkritiska systemdelar (single points of failure) och ***alltid*** kunna kontaktas och kontakta andra på flera olika sätt. Kommunikationskanalerna ska vara tydligt

specificerade och välkända för användargruppen och samarbetspartner.	specificerade och välkända för användargruppen och samarbetspartner.

Ändringsförslag 95

Förslag till direktiv
Bilaga I – led 1 – led c

Kommissionens förslag	*Ändringsförslag*
(c) ***Incidenthanteringsorganisationens*** kontor och de informationssystem som den använder sig av ska vara lokaliserade till säker plats.	(c) ***Incidenthanteringsorganisationernas*** kontor och de informationssystem som den använder sig av ska vara lokaliserade till säker plats ***med säkra nät och informationssystem***.

Ändringsförslag 96

Förslag till direktiv
Bilaga I – led 2 – led a – strecksats 1

Kommissionens förslag	*Ändringsförslag*
– Övervakning av incidenter på nationell nivå.	– ***Upptäckt och*** övervakning av incidenter på nationell nivå.

Ändringsförslag 97

Förslag till direktiv
Bilaga I – led 2 – led a – strecksats 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	– Aktivt delta i samarbetsnätverk för incidenthanteringsorganisationer på EU-nivå och internationell nivå

Ändringsförslag 98

Förslag till direktiv
Bilaga II

Kommissionens förslag	*Ändringsförslag*
Lista över marknadsoperatörer	Lista över marknadsoperatörer
1. Energi.	1. Energi.
	(a) Elektricitet.
	– Leverantörer.
	– Systemansvariga för distributionssystem och återförsäljare till slutkunderna.
	–Systemansvariga för överföringssystem (el).
	– Elmarknadsoperatörer.
	(b) Olja.
	– Oljeledningar och oljelager.
	– Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring.
	(c) Gas.
	– Leverantörer.
	– Systemansvariga för distributionssystem och återförsäljare till slutkunderna.
	– Systemansvariga för gasöverföringssystem, naturgaslager och LNG.
	– Operatörer av naturgasproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring.
	– Gasmarknadsoperatörer.
2. Transporter.	2. Transporter.
	(a) Vägtransport.
	(i) Trafikstyrning och trafikledning.
	(ii) Logistiska stödtjänster:
	– lager- och magasineringstjänster,
	– godshantering, och
	– andra stödverksamheter för transporter.
	(b) Järnvägstransport.
	(i) Järnväg (infrastrukturförvaltare, integrerade företag och

	järnvägstransportföretag).
	(ii) Trafikstyrning och trafikledning.
	(iii) Logistiska stödtjänster:
	– lager- och magasineringstjänster,
	– godshantering, och
	– andra stödverksamheter för transporter.
	(c) Lufttransport.
	(i) Lufttrafikföretag (gods- och persontransporter).
	(ii) Flygplatser.
	(iii) Operatörer inom flygledningss- och flygkontrolltjänster.
	(iv) Logistiska stödtjänster:
	– lagertjänster,
	– godshantering, och
	– andra stödverksamheter för transporter.
	(d) Sjötransporter.
	(i) Sjötransportföretag (transportföretag som bedriver persontrafik på inre vattenvägar, till havs och längs kuster samt transportföretag som bedriver godstrafik på inre vattenvägar, till havs och längs kuster).
	(ii) Hamnar
	(iii) Operatörer inom trafikledning- och trafikkontroll.
	(iv) Logistiska stödtjänster:
	– lager- och magasineringstjänster,
	– godshantering, och
	– andra stödverksamheter för transporter.
	2a. Vattentjänster.
3. Bankverksamhet: Kreditinstitut i enlighet med artikel 4.1 i direktiv 2006/48/EG.	3. Bankverksamhet: Kreditinstitut i enlighet med artikel 4.1 i direktiv 2006/48/EG.
4. Finansmarknadsinfrastruktur: ***börser*** och organisationer för central motpartsclearing.	4. Finansmarknadsinfrastruktur: ***reglerade marknader, multilaterala handelsplattformar, organiserade***

	handelsplattformar, internetbetalningsslussar och organisationer för central motpartsclearing.
5. Hälso- och sjukvårdssektorn: Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker) och andra enheter som tillhandahåller hälso- och sjukvårdsverksamhet.	5. Hälso- och sjukvårdssektorn: Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker) och andra enheter som tillhandahåller hälso- och sjukvårdsverksamhet.
	6. IKT: Molntjänster som används av en operatör för tillhandahållande av någon eller några av de tjänster som förtecknas i punkterna 1–5.
	Denna förteckning ska ses över vartannat år.

ÄRENDETS GÅNG

Titel	Hög allmän nivå av nät- och informationssäkerhet i EU
Referensnummer	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Ansvarigt utskott Tillkännagivande i kammaren	IMCO 15.4.2013
Yttrande från Tillkännagivande i kammaren	ITRE 15.4.2013
Associerat/associerade utskott - tillkännagivande i kammaren	12.9.2013
Föredragande av yttrande Utnämning	Pilar del Castillo Vera 23.5.2013
Behandling i utskott	14.10.2013 4.11.2013
Antagande	16.12.2013
Slutomröstning: resultat	+: 36 –: 5 0: 0
Slutomröstning: närvarande ledamöter	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Slutomröstning: närvarande suppleanter	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Slutomröstning: närvarande suppleanter (art. 187.2)	María Auxiliadora Correa Zamora

15.1.2014

YTTRANDE FRÅN UTSKOTTET FÖR MEDBORGERLIGA FRI- OCH RÄTTIGHETER SAMT RÄTTSLIGA OCH INRIKES FRÅGOR(*)

till utskottet för den inre marknaden och konsumentskydd

över förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Föredragande: Carl Schlyter

KORTFATTAD MOTIVERING

Förslaget syftar till att uppnå en hög gemensam nivå av nät- och informationssäkerhet i hela unionen. Föredraganden stöder förslagets mål och rekommenderar ändringsförslag som kommer att öka rättssäkerheten och stärka garantier och skydd för enskilda och deras integritet, för att se till att enskilda har kontroll över sina personuppgifter och litar på den digitala miljön, och för att skapa en kultur för riskhantering och förbättrat informationsutbyte mellan privata och offentliga parter.

De föreslagna ändringsförslagen avser att utöka hänvisningarna till uppgiftsskyddslagstiftningen, förtydliga att ”kritisk infrastruktur” inte bör omfatta sociala nätverk och onlineförsäljning av tillämpningar (se den ändrade förteckningen i bilaga II) och se till att proportionaliteten respekteras, genom att understryka den civila aspekten i ärendet. De flesta störningar och vanliga orsaker till systemfel är inte avsiktliga it-attacker som genomförs av terrorister, brottslingar eller utländska spioner, utan de är oavsiktliga och beror på mänskliga fel och naturliga orsaker. Det är av avgörande betydelse att EU gör skillnad mellan genomförandet av den föreslagna lagstiftningen och varje form av militarisering av ärendet, utesluter säkerhets- och övervakningsindustrins mål och beaktar det sammanhang som en globaliserad digital marknad utgör.

Ett stort kvarstående bekymmer är hur det föreslagna systemet förhåller sig till det meddelandesystem som föreslås enligt den allmänna uppgiftsskyddsförordningen, och hur dessa kan samexistera. Detta är ett av skälen till att vi understryker att all EU-lagstiftning om it-säkerhet bör följa på antagandet av den allmänna uppgiftsskyddsförordningen och inte föregå det. Vidare bör man beakta de verkliga finansiella och administrativa följderna, inklusive den sammanlagda kostnaden för samhället och inte bara kostnaden för ett meddelande. Programföretag som ägnar sig åt mindre noggrann programmering, och som

därmed sparar pengar genom att utsätta sina kunder för risker, kan inte i samtliga fall skyddas av den standardformulering i användarvillkoren där de friskriver sig från allt ansvar för tekniska fel i deras program. De måste få incitament för att se till att programmen är rimligt säkra. Vidare bör nyckelbegrepp förtydligas och inte lämnas öppna för medlemsstaternas tolkning (exempelvis betydelsen av begreppen ”offentliga förvaltningar” och ”betydande inverkan” samt en konkret definition av begreppet ”it-brottslighet”).

ÄNDRINGSFÖRSLAG

Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor uppmanar utskottet för den inre marknaden och konsumentskydd att som ansvarigt utskott infoga följande ändringsförslag i sitt betänkande:

Ändringsförslag 1

Förslag till direktiv
Skäl 1

Kommissionens förslag	*Ändringsförslag*
(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet ***och*** social välfärd och ***i synnerhet för den inre marknadens funktion***.	(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet***,*** social välfärd och ***kommunikation och utbyten mellan personer, organisationer inom civilsamhället och företag samt för skydd av och respekt för integritet och personuppgifter***.

Ändringsförslag 2

Förslag till direktiv
Skäl 2

Kommissionens förslag	*Ändringsförslag*
(2) Avsiktliga eller oavsiktliga säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens	(2) Avsiktliga eller oavsiktliga säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens

funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.	funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi. ***Allt fler inser nu att kontrollsystemen är sårbara för it-attacker från bland annat fientliga regeringar, terroristgrupper och andra illasinnade inkräktare. Smarta och samordnade attacker kan allvarligt skada infrastrukturens stabilitet, prestanda och ekonomi.***

Ändringsförslag 3

Förslag till direktiv
Skäl 3

Kommissionens förslag	*Ändringsförslag*
(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad.	(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad ***och för kommunikation och utbyten mellan personer, organisationer inom civilsamhället och företag***.

Ändringsförslag 4

Förslag till direktiv
Skäl 3a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(3a) Eftersom de vanligare orsakerna till systemfel fortsatt är oavsiktliga,

	exempelvis naturliga orsaker eller mänskliga fel, bör infrastrukturen kunna stå emot både avsiktliga och oavsiktliga störningar, och operatörer som driver kritisk infrastruktur bör utforma motståndskraftsbaserade system som fungerar även när andra system utanför deras kontroll inte fungerar.

Ändringsförslag 5

Förslag till direktiv
Skäl 6a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(6a) Det är viktigt att inse den inneboende osäkerheten hos de komplexa system som omger oss. Detta kräver en bättre gemensam uppfattning om vad som är viktigt bland dem som skyddar en organisation och de som fastställer dess strategiska inriktning.

Ändringsförslag 6

Förslag till direktiv
Skäl 8

Kommissionens förslag	*Ändringsförslag*
(8) Bestämmelserna i detta direktiv bör inte påverka varje enskild medlemsstats möjligheter att vidta de åtgärder som är nödvändiga för att skydda sina väsentliga säkerhetsintressen, för att skydda allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och åtal av brott. Enligt artikel 346 i EUF-fördraget ska ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.	(8) Bestämmelserna i detta direktiv bör inte påverka varje enskild medlemsstats möjligheter att vidta de åtgärder som är nödvändiga för att skydda sina väsentliga säkerhetsintressen, för att skydda allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och åtal av brott***, förutsatt att de inte använder detta som förevändning för att inte fullgöra sina mer allmänna skyldigheter att respektera skyddet av integritet och personuppgifter***. Enligt artikel 346 i EUF-fördraget ska ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga

säkerhetsintressen.

Ändringsförslag 7

Förslag till direktiv
Skäl 9

Kommissionens förslag	*Ändringsförslag*
(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå utarbeta planer för samarbete om nät- och informationssäkerhet med grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter.	(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå utarbeta planer för samarbete om nät- och informationssäkerhet med grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter***,*** ***samtidigt som man respekterar och skyddar integriteten och personuppgifter***.

Ändringsförslag 8

Förslag till direktiv
Skäl 10

Kommissionens förslag	*Ändringsförslag*
(10) För att uppnå ett effektivt genomförande av de bestämmelser som antas i enlighet med detta direktiv bör man i varje medlemsstat inrätta eller utse ***ett organ*** med ansvar för samordning av nät- och informationssäkerhetsfrågor som kan fungera som sambandspunkt för det gränsöverskridande samarbetet på unionsnivå. Dessa organ bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå detta	(10) För att uppnå ett effektivt genomförande av de bestämmelser som antas i enlighet med detta direktiv bör man i varje medlemsstat inrätta eller utse ***en nationell behörig myndighet under civil kontroll och med fullständig demokratisk tillsyn som har insyn i verksamheten*** med ansvar för samordning av nät- och informationssäkerhetsfrågor som kan fungera som sambandspunkt för det gränsöverskridande samarbetet på unionsnivå. Dessa organ bör förses med de tekniska och finansiella resurser och

direktivs mål.

personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå detta direktivs mål.

Ändringsförslag 9

Förslag till direktiv
Skäl 14a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(14a) Allt fler sektorer inför molntjänster i sin datormiljö, t.ex. it-tjänster som driver kritisk infrastruktur. För att vara tillräckliga måste säkerhetsåtgärderna garantera sekretess, integritet och tillgänglighet för de uppgifter som hanteras i molnet. Att vara värd för infrastrukturtjänster och lagra känslig information i molnmiljön medför krav på säkerhet och driftsäkerhet som de nuvarande molntjänsterna har svårt att uppfylla. Därför krävs det garantier för att datatjänsterna i molnmiljön kan erbjuda ett tillräckligt skydd för känslig information om kritisk infrastruktur genom utveckling av innovativ teknik för att upptäcka intrång.

Ändringsförslag 10

Förslag till direktiv
Skäl 15

Kommissionens förslag	*Ändringsförslag*
(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor. Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och	(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor. Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och

utbyta information och bästa praxis ***i utbyte mot*** operativt stöd vid incidenter.	***sinsemellan*** utbyta information och bästa praxis ***samt vid behov erbjuda ömsesidigt*** operativt stöd vid incidenter.

Ändringsförslag 11

Förslag till direktiv
Skäl 15a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(15a) Redan befintliga nationella mekanismer för samarbete mellan offentliga och privata operatörer bör om möjligt respekteras fullt ut och i enlighet med direktiv 95/46/EG, och de bestämmelser som anges i detta direktiv bör inte undergräva sådana etablerade samarbetsarrangemang.

Ändringsförslag 12

Förslag till direktiv
Skäl 16

Kommissionens förslag	*Ändringsförslag*
(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de behöriga myndigheterna skapa en gemensam webbplats för offentliggörande av sådan information om incidenter och risker som inte är konfidentiell.	(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de behöriga myndigheterna skapa en gemensam webbplats för ***snabbt och uttömmande*** offentliggörande av sådan information om incidenter och risker som inte är konfidentiell.

Ändringsförslag 13

Förslag till direktiv
Skäl 21

Kommissionens förslag	*Ändringsförslag*
(21) I och med att nät- och informationssäkerhetsproblemen är globala	(21) I och med att nät- och informationssäkerhetsproblemen är globala

till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyten och främja ett gemensamt sätt att hantera nät- och informationssäkerhetsfrågor.

till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyten och främja ett gemensamt sätt att hantera nät- och informationssäkerhetsfrågor***, förutsatt att de stater med vilka sådant samarbete planeras besitter instrument för kontroll och skydd av uppgifter som garanterar samma säkerhet som EU:s motsvarande instrument***.

Ändringsförslag 14

Förslag till direktiv
Skäl 22

Kommissionens förslag	*Ändringsförslag*
(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på offentliga förvaltningar och ***marknadsoperatörer***. En kultur av riskhantering, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som ***är anpassade till riskerna***, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Lika konkurrensvillkor för alla krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.	(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på offentliga förvaltningar och ***företag***. En kultur av riskhantering, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som ***syftar till att föregripa avsiktliga och oavsiktliga säkerhetsincidenter***, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. ***I de fall där en sådan kultur av riskhantering redan finns, och framför allt där den bygger på frivilliga rutiner, bör den stödjas, stärkas och spridas.*** Lika konkurrensvillkor för alla krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.

Ändringsförslag 15

Förslag till direktiv
Skäl 22a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(22a) Offentliga förvaltningar och privata företag, inklusive leverantörer av tjänster inom nät, information och programvara, bör betrakta skyddet av sina informationssystem och de uppgifter som dessa innehåller som en del av sin omsorgsplikt. En lämplig skyddsnivå bör garanteras mot hot och sårbarheter som rimligen kan identifieras. De kostnader och bördor som ett sådant skydd medför bör spegla den skada som ett it-angrepp skulle kunna orsaka för de drabbade personerna.

Ändringsförslag 16

Förslag till direktiv
Skäl 26a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(26a) Barn exponeras mycket tidigt för internet och annan modern teknik samt de hot som detta medför. Goda vägledande principer för barnvänliga zoner på internet är avgörande för att kunna minska skadorna och garantera att skyddet av barnen och deras rättigheter inte äventyras.

Ändringsförslag 17

Förslag till direktiv
Skäl 28

Kommissionens förslag	*Ändringsförslag*
(28) Behöriga myndigheter bör se till att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. Vid offentliggörande av incidenter som rapporteras till de behöriga	(28) Behöriga myndigheter bör se till att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. Vid offentliggörande av incidenter som rapporteras till de behöriga

myndigheterna bör allmänhetens intresse av att få information om hot ***vägas mot eventuella negativ inverkan på ryktet och affärerna för de offentliga förvaltningar och marknadsoperatörer som rapporterar incidenter. Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar släpps***.	myndigheterna bör allmänhetens intresse av att få information om hot ***prioriteras högre än kortsiktiga ekonomiska överväganden***.

Ändringsförslag 18

Förslag till direktiv
Skäl 29a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(29a) Genom att utnyttja internet i kriminell verksamhet kan den organiserade brottsligheten utöka sin verksamhet inom penningtvätt och förfalskning och när det gäller andra produkter och tjänster som kränker den immateriella äganderätten samt för att experimentera med nya kriminella verksamheter, vilket avslöjar en skrämmande förmåga att utnyttja den moderna tekniken.

Ändringsförslag 19

Förslag till direktiv
Skäl 30a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(30a) It-brott orsakar allt allvarligare ekonomiska och sociala skador som drabbar miljontals konsumenter, med förluster som uppskattas till 290 miljarder euro per år[4a].

[4a] Enligt Nortons rapport om it-brott 2012.

Ändringsförslag 20

Förslag till direktiv
Skäl 33

Kommissionens förslag	*Ändringsförslag*
(33) Detta direktiv bör ses över med jämna mellanrum, främst i syfte att avgöra behovet av modifieringar med hänsyn till den tekniska utvecklingen eller ändrade marknadsvillkor.	(33) Detta direktiv bör ses över ***av kommissionen*** med jämna mellanrum, främst i syfte att avgöra behovet av modifieringar med hänsyn till den tekniska utvecklingen eller ändrade marknadsvillkor ***och skyldigheter som syftar till högsta nivå av säkerhet och integritet för nät och information samt skydd av privatliv och personuppgifter***.

Ändringsförslag 21

Förslag till direktiv
Skäl 39

Kommissionens förslag	*Ändringsförslag*
(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse ***och är därmed*** berättigad enligt artikel 7 i direktiv 95/46/EG. ***I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i*** rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till	(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna kan förutsätta behandling av personuppgifter. ***Om*** sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse ***kan den vara*** berättigad enligt artikel 7 i direktiv 95/46/EG. ***Detta undantar dock inte de behöriga myndigheterna från kravet att ett ingripande måste vara proportionerligt och inte får kränka*** rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till

Europaparlamentets, rådets och kommissionens handlingar[8] gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.	Europaparlamentets, rådets och kommissionens handlingar gälla i tillämpliga fall[8]. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.
[8] EGT L 145, 31.5.2001, s. 43.	[8] EGT L 145, 31.5.2001, s. 43.

Ändringsförslag 22

Förslag till direktiv
Skäl 41a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(41a) Vid alla åtgärder måste skyddet av grundläggande mänskliga rättigheter, särskilt de rättigheter som anges i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (artikel 8, privat- och familjeliv) säkerställas och överensstämmelsen med proportionalitetsprincipen garanteras.

Ändringsförslag 23

Förslag till direktiv
Artikel 1 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. Detta direktiv ***påverkar inte heller tillämpningen av*** Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter	5. Detta direktiv ***ska till fullo respektera*** Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om

och om det fria flödet av sådana uppgifter och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och Europaparlamentets och rådets förordning om skydd för enskilda ***personer med avseende på behandling av*** personuppgifter och om ***det*** fria ***flödet av*** sådana uppgifter.

det fria flödet av sådana uppgifter och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och Europaparlamentets och rådets förordning ***(EG) nr 45/2001 av den 18 december 2000*** om skydd för enskilda ***då gemenskapsinstitutionerna och gemenskapsorganen behandlar*** personuppgifter och om ***den*** fria ***rörligheten för*** sådana uppgifter.

Ändringsförslag 24

Förslag till direktiv
Artikel 2

Kommissionens förslag	*Ändringsförslag*
Medlemsstaterna ska inte vara förhindrade att anta eller behålla bestämmelser som garanterar en högre säkerhetsnivå, utan att det påverkar deras skyldigheter enligt unionslagstiftningen.	Medlemsstaterna ska inte vara förhindrade att anta eller behålla bestämmelser som garanterar en högre säkerhetsnivå, utan att det påverkar deras skyldigheter enligt unionslagstiftningen***, men bestämmelserna måste uppfylla de gemensamma minimikrav som anges i detta direktiv***.

Ändringsförslag 25

Förslag till direktiv
Artikel 3 – led 2

Kommissionens förslag	*Ändringsförslag*
(2) säkerhet: förmågan hos ett nät eller ett informationssystem att***, vid en viss tillförlitlighetsnivå,*** tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga	(2) säkerhet: förmågan hos ett nät eller ett informationssystem att tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem.

via dessa nät och informationssystem.

Ändringsförslag 26

Förslag till direktiv
Artikel 3 – punkt 2 – led a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(a) it-beredskap: förmågan hos ett nät eller ett informationssystem att stå emot och återgå till full operativ kapacitet efter incidenter, inklusive – men inte begränsade till – tekniska fel, strömavbrott och säkerhetsrelaterade incidenter.

Ändringsförslag 27

Förslag till direktiv
Artikel 3 – led 4

Kommissionens förslag	*Ändringsförslag*
(4) incident: en omständighet eller händelse som har en faktisk negativ inverkan på säkerheten.	(4) incident: en omständighet eller händelse som har en faktisk negativ inverkan på säkerheten ***och tillhandahållandet av kärntjänster***.

Ändringsförslag 28

Förslag till direktiv
Artikel 3 – led 8 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ***ekonomisk*** och ***samhällelig*** verksamhet inom områdena energi-, transport-, bank-, börs- samt hälso- och sjukvårdsverksamhet; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II.	(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ***samhällelig*** och ***ekonomisk*** verksamhet inom områdena energi-, transport-, bank-, börs***-, livsmedelskedje-*** samt hälso- och sjukvårdsverksamhet; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II.

Ändringsförslag 29

Förslag till direktiv
Artikel 5 – punkt 2 – led a

Kommissionens förslag	*Ändringsförslag*
(a) En ***riskbedömningsplan*** för kartläggning av risker och bedömning av verkningarna av potentiella incidenter.	(a) En ***ram*** för ***riskhantering som åtminstone omfattar en regelbunden utvärdering av risker som möjliggör*** kartläggning av risker och bedömning av verkningarna av potentiella incidenter***, samt åtgärder för att garantera säkerhet, integritet och uppgifter, inklusive ett system för tidig varning***.

Motivering

En riskbedömningsplan räcker inte och omfattar inte andra nödvändiga åtgärder för riskhantering i fråga om nät- och informationssäkerhet. Europeiska datatillsynsmannen rekommenderar inrättandet av en ram för riskhantering som omfattar utvärdering av riskerna.

Ändringsförslag 30

Förslag till direktiv
Artikel 5 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Den nationella NIS-strategin och den nationella NIS-samarbetsplanen ska meddelas kommissionen inom en månad från antagandet.	3. Den nationella NIS-strategin och den nationella NIS-samarbetsplanen ska meddelas kommissionen***, Europaparlamentet och Europeiska datatillsynsmannen*** inom en månad från antagandet***, vilket ska ske senast 12 månader efter detta direktivs ikraftträdande***.

Ändringsförslag 31

Förslag till direktiv
Artikel 5 – punkt 3a (ny)

Kommissionens förslag	*Ändringsförslag*
	3a. Kommissionen ska efter att ha samlat in varje medlemsstats nationella nät- och informationssäkerhetsstrategi på ett organiserat sätt förmedla dessa till varje medlemsstat.

Motivering

Det är av värde att medlemsstaterna får ta del av varandras planer. Det är till hjälp i anpassningen och kan även bidra till utbytet av bästa praxis.

Ändringsförslag 32

Förslag till direktiv
Artikel 5 – punkt 3b (ny)

Kommissionens förslag	*Ändringsförslag*
	3b. Kommissionen ska sammanställa den nationella nät- och informationssäkerhetsstrategins struktur senast sex månader efter det att föreliggande förordning har antagits. Målet ska vara att hjälpa medlemsstaterna att utarbeta och anta dokument med liknande struktur.

Motivering

På unionsnivå kan man på ett mer verksamt sätt organisera och anpassa 28 dokument om de har en liknande struktur. Kommissionens riktlinjer skulle visserligen inte vara bindande, men skulle ändå leda till att medlemsstaterna vid utarbetandet av de egna strategierna skulle följa denna föreslagna modell eller struktur.

Ändringsförslag 33

Förslag till direktiv
Artikel 6 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska utse en behörig nationell myndighet för säkerheten i nät	1. Varje medlemsstat ska utse en behörig ***civil*** nationell myndighet för säkerheten i

och informationssystem (den behöriga myndigheten).	nät och informationssystem (den behöriga myndigheten).

Ändringsförslag 34

Förslag till direktiv
Artikel 6 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. De behöriga myndigheterna ska när så är lämpligt samråda och ***samarbeta*** med de ***relevanta*** nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.	5. De behöriga myndigheterna ska när så är lämpligt ***och med beaktande av proportionalitetsprincipen*** samråda och ***föra ett nära samarbete*** med de ***behöriga*** nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.

Ändringsförslag 35

Förslag till direktiv
Artikel 6 – punkt 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	5a. Med avseende på den information som samlas in, behandlas och utbyts ska de behöriga myndigheterna uppfylla de krav på skydd av personuppgifter som fastställs i artikel 17 i direktiv 95/46/EG.

Ändringsförslag 36

Förslag till direktiv
Artikel 7 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska inrätta ***en incidenthanteringsorganisation*** (Computer Emergency Response ***Team***, ***Cert***) som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation ***får*** inrättas	1. Varje medlemsstat ska inrätta ***incidenthanteringsorganisationer*** (Computer Emergency Response ***Teams***, ***Certs***) som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. ***Vid behov ska*** en

inom den behöriga myndigheten.	incidenthanteringsorganisation inrättas inom den behöriga myndigheten.

Ändringsförslag 37

Förslag till direktiv
Artikel 8 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Samarbetsnätverket ska föra samman kommissionen och de behöriga myndigheterna i kontinuerlig kommunikation. På begäran ska Europeiska byrån för nät- och informationssäkerhet (Enisa) bistå samarbetsnätverket med ***expertis och råd***.	2. Samarbetsnätverket ska föra samman kommissionen och de behöriga myndigheterna i kontinuerlig kommunikation. På begäran ska Europeiska byrån för nät- och informationssäkerhet (Enisa) bistå samarbetsnätverket med ***teknikneutral vägledning om åtgärder som är lämpliga för såväl offentliga som privata sektorer***.

Ändringsförslag 38

Förslag till direktiv
Artikel 9 – punkt 2 – led ba (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ba) Det ska finnas kriterier för medlemsstaternas deltagande i det säkra systemet för informationsutbyte, för att se till att en hög säkerhets- och beredskapsnivå garanteras av alla deltagare och i alla steg av behandlingen, bland annat genom sådana lämpliga åtgärder för sekretess och säkerhet som avses i artiklarna 16 och 17 i direktiv 95/46/EG och i artiklarna 21 och 22 i förordning (EG) nr 45/2001.

Ändringsförslag 39

Förslag till direktiv
Artikel 9 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Kommissionen ska genom genomförandeakter besluta om medlemsstaternas tillträde till denna säkra infrastruktur, i enlighet med de kriterier som avses i punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.3.	***utgår***

Ändringsförslag 40

Förslag till direktiv
Artikel 12 – punkt 2 – led a – strecksats 2

Kommissionens förslag	*Ändringsförslag*
– En definition av ***förfarandena och*** kriterierna för samarbetsnätverkets bedömning av risker och incidenter.	– En definition av kriterierna för samarbetsnätverkets bedömning av risker och incidenter.

Ändringsförslag 41

Förslag till direktiv
Artikel 13

Kommissionens förslag	*Ändringsförslag*
Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. Sådana avtal ***ska beakta behovet av ändamålsenligt*** skydd för personuppgifter som förmedlas via samarbetsnätverket.	Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. Sådana avtal ***får endast ingås om ett*** skydd för personuppgifter som förmedlas via samarbetsnätverket ***kan garanteras som är tillräckligt och jämförbart med det skydd som garanteras i EU***.

Ändringsförslag 42

Förslag till direktiv
Artikel 14 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Medlemsstaterna ska se till att offentliga förvaltningar och marknadsoperatörer vidtar ändamålsenliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten för de nät och informationssystem som de kontroller och använder i sin verksamhet. Med beaktande av den senaste tekniken ska dessa åtgärder garantera en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga och minimera de effekter som incidenter som påverkar deras nät och informationssystem har på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem.	1. Medlemsstaterna ska se till att offentliga förvaltningar och marknadsoperatörer vidtar ändamålsenliga tekniska och organisatoriska åtgärder för att ***upptäcka, effektivt*** hantera ***samt begränsa de*** risker som hotar säkerheten för de nät och informationssystem som de kontrollerar och använder i sin verksamhet. Med beaktande av den senaste tekniken ska dessa åtgärder garantera en säkerhetsnivå som är anpassad ***och proportionerlig i förhållande*** till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga och minimera de effekter som incidenter som påverkar deras nät och informationssystem har på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten ***samt datasäkerheten*** för de tjänster som använder dessa nät och informationssystem.

Ändringsförslag 43

Förslag till direktiv
Artikel 14 – punkt 2 – led a (nytt)

	Ändringsförslag
	(a) Kommersiella programvarutillverkare ska hållas ansvariga vid en eventuell allvarlig försummelse som gäller skydd och säkerhet, trots klausuler om ansvarsfrihet i brukaravtalen.

Motivering

I licensavtalet fritar de kommersiella programvarutillverkarna sig själva från allt eventuellt ansvar på grund av oaktsamhet i samband med säkerhet och dålig programmering. För att förmå programvarutillverkarna att investera i säkerhetsåtgärder krävs det en annan kultur.

Den kan enbart förverkligas om programvarutillverkarna hålls ansvariga för alla säkerhetsbrister.

Ändringsförslag 44

Förslag till direktiv
Artikel 14 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. Dessa krav enligt punkterna 1 och 2 gäller för alla marknadsoperatörer som tillhandahåller tjänster inom Europeiska unionen.	3. Dessa krav enligt punkterna 1 och 2 gäller för alla marknadsoperatörer ***och programtillverkare*** som tillhandahåller tjänster inom Europeiska unionen.

Ändringsförslag 45

Förslag till direktiv
Artikel 14 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. Utan att det påverkar tillämpningen av delegerade akter som antas enligt punkt 5 får de behöriga myndigheterna anta riktlinjer och, om nödvändigt, utfärda anvisningar avseende de omständigheter då offentliga förvaltningar och marknadsoperatörer är skyldiga att anmäla incidenter.	***utgår***

Ändringsförslag 46

Förslag till direktiv
Artikel 15 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter ***de behöver*** för att utreda fall då offentliga förvaltningar eller marknadsoperatörer inte uppfyllt sina skyldigheter enligt artikel 14 och de effekter som detta har på nätens och	1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter ***som behövs*** för att utreda fall då offentliga förvaltningar eller marknadsoperatörer inte uppfyllt sina skyldigheter enligt artikel 14 och de effekter som detta har på nätens och

informationssystemens säkerhet.	informationssystemens säkerhet.

Ändringsförslag 47

Förslag till direktiv
Artikel 15 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. De behöriga myndigheterna ***ska*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott.	5. ***Utan att det påverkar tillämplig dataskyddslagstiftning, och i fullt samråd med relevanta registeransvariga och registerförare, ska*** de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott.

Ändringsförslag 48

Förslag till direktiv
Artikel 19a (ny)

Kommissionens förslag	*Ändringsförslag*
	Artikel 19a
	Databehandling och dataskydd
	1. All behandling av personuppgifter i medlemsstaterna med tillämpning av detta direktiv ska ske i enlighet med direktiven 95/46/EG och 2002/58/EG.
	2. All behandling av personuppgifter som utförs av kommissionen och Enisa med tillämpning av detta direktiv ska ske i enlighet med förordning (EG) nr 45/2001.
	3. All behandling av personuppgifter som utförs av Europeiska it-brottscentrumet inom Europol med tillämpning av detta direktiv ska ske i enlighet med beslut 2009/371/RIF.
	4. Behandlingen av personuppgifter ska vara rättvis och laglig och ska begränsas till de minimiuppgifter som krävs för det

	syfte för vilket de behandlas. Personuppgifterna ska lagras på ett sätt som förhindrar identifiering av de registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.
	5. De anmälningar av incidenter som avses i artikel 14 ska inte påverka tillämpningen av de bestämmelser och skyldigheter i fråga om att anmäla personuppgiftsbrott som fastställs i artikel 4 i direktiv 2002/58/EG och i förordning (EU) nr 611/2013.
	6. Hänvisningar till direktiv 95/46/EG ska tolkas som hänvisningar till Europaparlamentets och rådets förordning om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (den allmänna uppgiftsskyddsförordningen) när den har trätt i kraft.

Ändringsförslag 49

Förslag till direktiv
Artikel 20

Kommissionens förslag	*Ändringsförslag*
Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast ***tre*** år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.	Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast ***två*** år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.

Ändringsförslag 50

Förslag till direktiv
Bilaga I – stycke 1 – led 1 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Incidenthanteringsorganisationen ska genomföra och förvalta säkerhetsåtgärder för att säkra konfidentialiteten, integriteten, åtkomligheten och äktheten för den information som den får in och behandlar.	(b) Incidenthanteringsorganisationen ska genomföra och förvalta säkerhetsåtgärder för att säkra konfidentialiteten, integriteten, åtkomligheten och äktheten för den information som den får in och behandlar ***och för att säkerställa att personuppgifter skyddas***.

Ändringsförslag 51

Förslag till direktiv
Bilaga II – stycke 1

Kommissionens förslag	*Ändringsförslag*
Lista över marknadsoperatörer	Lista över marknadsoperatörer
Enligt artikel 3.8 a:	Enligt artikel 3.8 a:
1. E-handelsplattformar.	1. E-handelsplattformar.
2. Internetbetalningsslussar.	2. Internetbetalningsslussar.
3. Sociala medier.	
4. Sökmotorer	***3***. Sökmotorer
5. Molntjänster.	***4.*** Molndatatjänster ***som lagrar EU:s känsliga information om kritisk infrastruktur***.
6. Onlineförsäljning av tillämpningar.	

Ändringsförslag 52

Förslag till direktiv
Bilaga II – stycke 2 – punkt 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	5a. Livsmedelskedjan.

ÄRENDETS GÅNG

Titel	Hög allmän nivå av nät- och informationssäkerhet i EU			
Referensnummer	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Ansvarigt utskott Tillkännagivande i kammaren	IMCO 15.4.2013			
Yttrande från Tillkännagivande i kammaren	LIBE 15.4.2013			
Associerat/associerade utskott - tillkännagivande i kammaren	12.9.2013			
Föredragande av yttrande Utnämning	Carl Schlyter 7.3.2013			
Behandling i utskott	25.4.2013	18.9.2013	4.11.2013	13.1.2014
Antagande	13.1.2014			
Slutomröstning: resultat	+: –: 0:	36 6 0		
Slutomröstning: närvarande ledamöter	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in ‘t Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Slutomröstning: närvarande suppleanter	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
Slutomröstning: närvarande suppleanter (art. 187.2)	Katarína Neveďalová			

6.12.2013

YTTRANDE FRÅN UTSKOTTET FÖR UTRIKESFRÅGOR

till utskottet för den inre marknaden och konsumentskydd

över förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Föredragande: Ana Gomes

ÄNDRINGSFÖRSLAG

Utskottet för utrikesfrågor uppmanar utskottet för den inre marknaden och konsumentskydd att som ansvarigt utskott infoga följande ändringsförslag i sitt betänkande:

Ändringsförslag 1

Förslag till direktiv
Skäl 1

Kommissionens förslag	*Ändringsförslag*
(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion.	(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion ***och EU:s yttre säkerhet***.

Ändringsförslag 2

Förslag till direktiv
Skäl 2

Kommissionens förslag	*Ändringsförslag*
(2) Avsiktliga eller oavsiktliga säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.	(2) Avsiktliga eller oavsiktliga säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi ***samt i slutändan hota EU-medborgarnas välbefinnande och EU-medlemsstaternas förmåga att skydda sig själva och garantera säkerheten för kritiska infrastrukturer***.

Ändringsförslag 3

Förslag till direktiv
Skäl 2a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(2a) Solidaritetsklausulen, som införts genom artikel 222 i EUF-fördraget, utgör den lämpliga ramen för bistånd och gemensamt handlande bland EU:s medlemsstater i fall av terroristattacker eller kriminell verksamhet som hotar nät- och informationssäkerheten. På samma sätt ska klausulen om ömsesidigt försvar i artikel 42.7 i EU-fördraget utgöra ramen för handlande inom EU om en medlemsstat skulle utsättas för ett väpnat angrepp som skadar nät- och informationssäkerheten. Artikel 222 i EUF-fördraget och artikel 42.7 i EU-fördraget bör tillämpas så att de kompletterar varandra i fall där detta är lämpligt.

Ändringsförslag 4

Förslag till direktiv
Skäl 2a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(2a) Ett stort antal it-incidenter inträffar till följd av att den privata och offentliga nätinfrastrukturen inte är tillräckligt motståndskraftig och tålig, databaserna är dåligt skyddade eller säkrade och andra brister förekommer i den kritiska informationsinfrastrukturen. Endast ett fåtal medlemsstater anser att det ingår i respektive aktsamhetskrav att skydda sina nät och informationssystem och uppgifterna i dem, och detta förklarar bristen på investeringar i den senaste säkerhetstekniken samt i utbildning och utveckling av lämpliga riktlinjer.

Ändringsförslag 5

Förslag till direktiv
Skäl 3

Kommissionens förslag	*Ändringsförslag*
(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad.	(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad ***och för EU:s inre och yttre säkerhet***. ***Behovet att förbättra nät- och informationssäkerheten bör därför framhållas på lämpligt sätt i unionens strategi för inre säkerhet och***

***den europeiska säkerhetsstrategin, särskilt med tanke på den kommande översynen av dessa dokument*.**

Ändringsförslag 6

Förslag till direktiv
Skäl 3a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(3a) Att öka medvetenheten och utbilda dem som använder informations- och kommunikationsteknik i fråga om bästa metoder för att skydda personuppgifter och på ett hållbart sätt underhålla kommunikationstjänster bör utgöra grunden för alla övergripande it-säkerhetsstrategier.

Ändringsförslag 7

Förslag till direktiv
Skäl 4a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4a) Samarbete och samordning mellan de relevanta europeiska myndigheterna, vice ordföranden för kommissionen/den höga representanten – med ansvar för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken – och EU:s samordnare för kampen mot terrorism bör garanteras i samtliga fall där det kan förefalla finnas risker i form av yttre hot och terroristverksamhet.

Ändringsförslag 8

Förslag till direktiv
Skäl 4b (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4b) Utbyte av underrättelseuppgifter och känslig information mellan medlemsstaterna och även mellan medlemsstaterna och de berörda behöriga unionsmyndigheterna bör stärkas och förankras i principerna om förtroende, solidaritet och samarbete. Varje handlingsplan för att förbättra nät- och systemsäkerheten bör därför till fullo utnyttja redan befintliga strukturer inom EU, såsom Sitcen och EU Intcen, och garantera samordning mellan alla strukturer av relevans för informationssäkerhet som är av betydelse för EU:s inre och yttre säkerhet.

Ändringsförslag 9

Förslag till direktiv
Skäl 4c (nytt)

Kommissionens förslag	*Ändringsförslag*
	(4c) Samarbete och informationsutbyte på global nivå, med relevanta internationella partner, är avgörande för en effektiv it-säkerhetsstrategi och för kraftfulla åtgärder som syftar till att förbättra nät- och informationssäkerheten inom EU, mot bakgrund av hotens gränsöverskridande karaktär.

Ändringsförslag 10

Förslag till direktiv
Skäl 8a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(8a) Säkerhetsåtgärder måste respektera de grundläggande rättigheter som artiklarna 2, 6 och 21 i EUF-fördraget ålägger EU och dess medlemsstater att respektera, såsom yttrandefriheten, uppgiftsskyddet och rätten till personlig integritet. Rätten till personlig integritet och uppgiftsskydd fastställs i EU:s stadga om de grundläggande rättigheterna och artikel 16 i EUF-fördraget.

Ändringsförslag 11

Förslag till direktiv
Skäl 11a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11a) Alla medlemsstater bör inrikta de nationella strategierna för it-säkerhet på skyddet av informationssystem och uppgifterna i dessa samt betrakta skyddet av denna kritiska infrastruktur som en del av respektive aktsamhetskrav. Alla medlemsstater bör anta och genomföra strategier, riktlinjer och instrument som erbjuder ett rimligt skydd mot rimligt identifierbara hot, så att de kostnader och bördor som skyddet medför står i proportion till den sannolika skadan hos de berörda parterna. Alla medlemsstater bör även vidta lämpliga åtgärder för att ålägga juridiska personer inom sin jurisdiktion att skydda personuppgifter som finns hos dem.

Ändringsförslag 12

Förslag till direktiv
Skäl 16

Kommissionens förslag	*Ändringsförslag*
(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de behöriga myndigheterna skapa en gemensam webbplats för offentliggörande av sådan information om incidenter och risker som inte är konfidentiell.	(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de behöriga myndigheterna skapa en gemensam webbplats för offentliggörande av sådan information om incidenter och risker som inte är konfidentiell. ***Personuppgifter som offentliggörs på denna webbplats bör begränsas till vad som är nödvändigt samt vara så anonyma som möjligt.***

Ändringsförslag 13

Förslag till direktiv
Skäl 30a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(30a) Detta direktiv påverkar inte unionens regelverk om uppgiftsskydd. Personuppgifter som används i enlighet med bestämmelserna i detta direktiv bör begränsas till den minimiuppsättning personuppgifter som är absolut nödvändig, överföras endast till absolut nödvändiga aktörer och vara så anonyma som möjligt, om inte fullständigt anonyma.

Ändringsförslag 14

Förslag till direktiv
Skäl 32a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(32a) Det föreliggande direktivet (direktivet om nät- och informationssäkerhet) påverkar inte det faktum att det är nödvändigt att anta

unionslagstiftning om allmänt uppgiftsskydd.

Ändringsförslag 15

Förslag till direktiv
Skäl 34a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(34a) Det finns ett behov att på EU-nivå reglera försäljning, leverans, överföring och export till tredjeländer av utrustning eller programvara som främst är avsedd för övervakning eller avlyssning av kommunikation över internet och telefoni över mobila eller fasta nät, samt tillhandahållande av stöd för att installera, driva eller uppdatera sådan utrustning eller programvara. Snarast möjligt måste kommissionen utarbeta lagstiftning som hindrar europeiska företag att exportera sådana produkter med dubbla användningsområden till icke-demokratiska, auktoritära och repressiva regimer.

Ändringsförslag 16

Förslag till direktiv
Artikel 1 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad och effektiv hantering och samordnade och effektiva svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.	(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad***,*** effektiv ***och verkningsfull*** hantering och samordnade och effektiva svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.

Ändringsförslag 17

Förslag till direktiv
Artikel 3 – led 1 – led b

Kommissionens förslag	*Ändringsförslag*
(b) ***apparat eller*** en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlade uppgifter, samt	(b) en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlade uppgifter, samt

Ändringsförslag 18

Förslag till direktiv
Artikel 3 – led 2a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(2a) it-motståndskraft: förmågan hos ett nät eller informationssystem att stå emot och återgå till full operativ kapacitet efter incidenter, inklusive – men inte begränsade till – tekniska fel, strömavbrott och säkerhetsincidenter.

Ändringsförslag 19

Förslag till direktiv
Artikel 3 – led 8 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena energi-, transport-, bank-, börs- ***samt*** hälso- och sjukvårdsverksamhet; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II.	(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena energi-, transport-, bank-, börs-***,*** hälso- och sjukvårdsverksamhet ***samt säkerhet och försvar***; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II.

Ändringsförslag 20

Förslag till direktiv
Artikel 3 – led 8 – led ba (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ba) Leverantör av sådana apparater, nät och informationssystem som avses i led 1 – eller delar av dessa – och som är kritiska för en hög gemensam nivå av nät- och informationssäkerhet.

Ändringsförslag 21

Förslag till direktiv
Artikel 6 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska utse en behörig nationell myndighet för säkerheten i nät och informationssystem (den behöriga myndigheten).	1. Varje medlemsstat ska utse en behörig ***civil*** nationell myndighet för säkerheten i nät och informationssystem (den behöriga myndigheten).

Ändringsförslag 22

Förslag till direktiv
Artikel 7 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Varje medlemsstat ska inrätta en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.	1. Varje medlemsstat ska inrätta ***minst*** en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.

Ändringsförslag 23

Förslag till direktiv
Artikel 8 – punkt 3 – led fa (nytt)

Kommissionens förslag	*Ändringsförslag*
	(fa) Om lämpligt med tanke på riskens eller hotets karaktär, informera EU:s samordnare för kampen mot terrorism, genom en rapport, och eventuellt uppmana nämnda samordnare att bistå i arbetet med analysen av de förberedande arbetena och åtgärderna från samarbetsnätverkets sida.

Ändringsförslag 24

Förslag till direktiv
Artikel 9 – punkt 1a (ny)

Kommissionens förslag	*Ändringsförslag*
	1a. Personuppgifter får göras tillgängliga endast för mottagare som behöver behandla uppgifterna för att utföra sina uppdrag i enlighet med en lämplig rättslig grund. De uppgifter som görs tillgängliga ska begränsas till vad som är nödvändigt för att mottagarna ska kunna utföra sina uppdrag. Det ska säkerställas att principen om ändamålsbegränsning följs. Tidsfristen för lagring av uppgifterna i fråga ska anges i enlighet med de syften som anges i detta direktiv.

Ändringsförslag 25

Förslag till direktiv
Artikel 10 – punkt 3

Kommissionens förslag	*Ändringsförslag*
3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att	3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att

en medlemsstat inkommer med relevant information om en specifik risk eller incident.	en medlemsstat inkommer med relevant information om en specifik risk eller incident***, i överensstämmelse med bestämmelserna i den allmänna uppgiftsskyddsförordningen***.

Ändringsförslag 26

Förslag till direktiv
Artikel 13 – punkt -1a (ny)

Kommissionens förslag	*Ändringsförslag*
	(-1a) Vice ordföranden för kommissionen/den höga representanten ska – särskilt med avseende på tredjeländer – integrera it-säkerhetsaspekterna i EU:s yttre åtgärder. Syftet ska vara att intensifiera erfarenhetsutbytet och samarbetet i fråga om it-säkerhet.

Ändringsförslag 27

Förslag till direktiv
Artikel 13 – punkt -1b (ny)

Kommissionens förslag	*Ändringsförslag*
	(-1b) Rådet och kommissionen ska inom ramen för sina förbindelser och samarbetsavtal med tredjeländer, särskilt de länder som är involverade i tekniksamarbete, understryka vikten av respekt för minimistandarderna när det gäller säkerheten för informationssystem.

Ändringsförslag 28

Förslag till direktiv
Artikel 20 – Rubriken

Kommissionens förslag	*Ändringsförslag*
Översyn	***Rapportering och*** översyn

Ändringsförslag 29

Förslag till direktiv
Artikel 20 – punkt -1a (ny)

Kommissionens förslag	*Ändringsförslag*
	(-1a) Kommissionen ska för Europaparlamentet och rådet lägga fram en årlig rapport om de incidenter och åtgärder som anmälts till den i enlighet med detta direktiv.

Ändringsförslag 30

Förslag till direktiv
Bilaga I – led 1 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Incidenthanteringsorganisationen ska genomföra och förvalta säkerhetsåtgärder för att säkra konfidentialiteten, integriteten, åtkomligheten och äktheten för den information som den får in och behandlar.	(b) Incidenthanteringsorganisationen ska genomföra och förvalta säkerhetsåtgärder för att säkra konfidentialiteten, integriteten, åtkomligheten och äktheten för den information som den får in och behandlar***, samtidigt som den följer uppgiftsskyddskraven***.

Ändringsförslag 31

Förslag till direktiv
Bilaga II – underrubrik 2 (enligt artikel 3.8 b) – punkt 5a (ny)

Kommissionens förslag	*Ändringsförslag*
	(5a) Säkerhets- och försvarssektorn:

Ekonomiska aktörer för byggentreprenad och tjänster som avses i direktiv 2009/81/EG, i synnerhet de som avses i artikel 46.

ÄRENDETS GÅNG

Titel	Hög allmän nivå av nät- och informationssäkerhet i EU
Referensnummer	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Ansvarigt utskott Tillkännagivande i kammaren	IMCO 15.4.2013
Yttrande från Tillkännagivande i kammaren	AFET 15.4.2013
Föredragande av yttrande Utnämning	Ana Gomes 19.2.2013
Behandling i utskott	18.9.2013
Antagande	5.12.2013
Slutomröstning: resultat	+: 31 –: 3 0: 8
Slutomröstning: närvarande ledamöter	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marietta Giannakou, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrey Kovatchev, Eduard Kukan, Marusya Lyubcheva, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
Slutomröstning: närvarande suppleanter	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
Slutomröstning: närvarande suppleanter (art. 187.2)	Hiltrud Breyer

ÄRENDETS GÅNG

Titel	Hög allmän nivå av nät- och informationssäkerhet i EU			
Referensnummer	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Framläggande för parlamentet	5.2.2013			
Ansvarigt utskott Tillkännagivande i kammaren	IMCO 15.4.2013			
Rådgivande utskott Tillkännagivande i kammaren	AFET 15.4.2013	INTA 15.4.2013	BUDG 15.4.2013	ECON 15.4.2013
	ENVI 15.4.2013	ITRE 15.4.2013	TRAN 15.4.2013	JURI 15.4.2013
	LIBE 15.4.2013			
Inget yttrande avges Beslut	INTA 20.3.2013	BUDG 21.2.2013	ECON 18.6.2013	ENVI 19.2.2013
	TRAN 18.3.2013	JURI 20.2.2013		
Associerat/associerade utskott Tillkännagivande i kammaren	ITRE 12.9.2013	LIBE 12.9.2013		
Föredragande Utnämning	Andreas Schwab 20.3.2013			
Behandling i utskott	25.4.2013	18.6.2013	5.9.2013	4.11.2013
	9.1.2014			
Antagande	23.1.2014			
Slutomröstning: resultat	+: –: 0:	33 1 1		
Slutomröstning: närvarande ledamöter	Claudette Abela Baldacchino, Pablo Arias Echeverría, Adam Bielan, Preslav Borissov, Sergio Gaetano Cofferati, Lara Comi, Anna Maria Corazza Bildt, Christian Engström, Vicente Miguel Garcés Ramón, Evelyne Gebhardt, Małgorzata Handzlik, Eduard-Raul Hellvig, Sandra Kalniete, Edvard Kožušník, Toine Manders, Hans-Peter Mayer, Franz Obermayr, Sirpa Pietikäinen, Zuzana Roithová, Heide Rühle, Andreas Schwab, Róża Gräfin von Thun und Hohenstein, Bernadette Vergnaud, Barbara Weiler			
Slutomröstning: närvarande suppleanter	Regina Bastos, Ashley Fox, María Irigoyen Pérez, Morten Løkkegaard, Tadeusz Ross, Marc Tarabella, Patricia van der Kammen, Sabine Verheyen, Josef Weidenholzer			
Slutomröstning: närvarande suppleanter (art. 187.2)	Vital Moreira, Oreste Rossi			
Ingivande	12.2.2014			