Europaparlamentet
2014-2019

Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

2017/0225(COD)

16.3.2018

YTTRANDE

från utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

till utskottet för industrifrågor, forskning och energi

över förslaget till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013 och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Föredragande av yttrande: Jan Philipp Albrecht

PA_Legam

KORTFATTAD MOTIVERING

Föredraganden välkomnar kommissionens förslag om en ”cybersäkerhetsakt”[1], eftersom det bättre definierar Enisas roll i det förändrade ekosystemet för it-säkerhet och tar fram åtgärder för standarder, certifiering och märkning på it-säkerhetsområdet med målet att göra IKT-baserade system, inbegripet uppkopplade enheter, säkrare.

Föredraganden anser dock att ytterligare förbättringar skulle kunna göras. Föredraganden är fast övertygad om att informationssäkerheten är av yttersta vikt för skyddet för medborgarnas grundläggande rättigheter enligt vad som fastställs i EU:s stadga om de grundläggande rättigheterna, liksom för kampen mot it-brottslighet och skyddet av demokratin och rättsstatsprincipen.

Grundläggande rättigheter: Osäkra system kan leda till dataintrång eller identitetsstöld som kan åstadkomma verklig skada och lidande för enskilda personer, inte minst utgöra en risk för deras liv, integritet, värdighet eller egendom. Exempelvis kan vittnen riskera att utsättas för hotelser och fysisk skada, och kvinnor riskerar att utsättas för våld i hemmet om deras hemadresser har lämnats ut. För sakernas internet, som också innehåller fysiska ställdon och inte bara sensorer, kan den fysiska integriteten och användarnas liv äventyras vid angrepp på informationssystem. De ändringar som föredraganden föreslår är framför allt inriktade på skyddet av artiklarna 1, 2, 3, 6, 7, 8, 11 och 17 i EU:s stadga om de grundläggande rättigheterna. Det finns även en framväxande konstitutionell rättspraxis som härleder en särskild grundläggande rätt till sekretess och integritet i it-system[2] utifrån det allmänna personlighetsskyddet, anpassat till dagens digitala värld.

Kampen mot cyberbrottsligheten: Vissa former av brott som begås på nätet, till exempel nätfiske eller finans- och bankbedrägeri, innebär ett missbruk av förtroende som inte kan motverkas genom åtgärder för cybersäkerhet – mot denna typ av brottslighet välkomnar föredraganden den föreslagna regelbundna uppsökande verksamheten och de allmänna upplysningskampanjer som riktas till slutanvändare och som anordnas av Enisa. Andra former av brottslighet på nätet omfattar angrepp på informationssystem, t.ex. hackning eller distribuerade överbelastningsattacker (DDoS), och mot denna typ av brottslighet anser föredraganden att en förhöjd it-säkerhet effektivt kommer att stärka kampen mot och förebyggande av cyberbrottslighet.

Demokrati och rättsstatsprincipen: Angrepp mot regeringars och icke-statliga aktörers it-system utgör ett tydligt och växande hot mot demokratin genom sin inblandning i fria och rättvisa val, till exempel genom att manipulera fakta och åsikter som påverkar hur medborgarna kommer att rösta, störa röstningen och förändra valresultatet eller undergräva förtroendet för valet.

Föredraganden föreslår därför i sitt förslag till LIBE:s yttrande att ändra kommissionens förslag och fokusera på följande viktiga frågor för LIBE-utskottet:

---

[1] Europeiska kommissionens förslag till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013 och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”), COM(2017)0477.

[2] Den tyska författningsdomstolens dom av den 27 februari 2008 i målen 1 BvR 370/07 och 1 BvR 595/07.

- Byrån bör spela en större roll när det gäller att främja att alla aktörer i det europeiska informationssamhället antar förebyggande och kraftfull integritetshöjande teknik och it-säkerhetsåtgärder.

- Byrån bör lägga fram strategier som fastställer tydliga uppgifter och ansvar för alla aktörer som deltar i IKT-ekosystem där underlåtenhet att agera med korrekt tillbörlig aktsamhet med avseende på it-säkerhet kan leda till svåra säkerhetskonsekvenser, massiv miljöförstörelse och utlösa en finansiell eller ekonomisk systemkris.

- Byrån bör lägga fram förslag på tydliga och obligatoriska grundläggande krav i fråga om it-säkerhet i samråd med experter på it-säkerhet.

- Byrån bör lägga fram ett system för it-säkerhetscertifiering som möjliggör för IKT-återförsäljare att öka insynen för konsumenterna om uppgraderingsmöjligheter och tider för programvarustöd. Ett sådant certifieringssystem måste vara dynamiskt eftersom säkerhet är en process som kräver ständig förbättring.

- Byrån bör göra det enklare och billigare för tillverkare av IKT-produkter att genomföra principer för inbyggd säkerhet genom att offentliggöra riktlinjer och bästa praxis.

- Byrån bör, på inbjudan av unionens institutioner, organ och byråer samt medlemsstaterna, regelbundet genomföra förebyggande granskningar av it-säkerheten i deras kritiska infrastruktur (rätt till revision).

- Byrån ska omedelbart rapportera brister i it-säkerheten som ännu inte är allmänt kända för tillverkare. Byrån får inte dölja eller utnyttja sekretessbelagda sårbarheter i företag och produkter för egna syften. Genom att utveckla, uppköpa och utnyttja bakdörrar i it-system med skattebetalarnas pengar sätter statliga organ medborgarnas säkerhet på spel. I syfte att skydda andra aktörer som hanterar sådana sårbarheter på ett ansvarsfullt sätt bör byrån föreslå strategier för ett ansvarsfullt utbyte av information om ”Zero days” och andra typer av säkerhetsbrister som ännu inte är allmänt kända och som underlättar avlägsnandet av sådana sårbarheter.

- För att göra det möjligt för EU att komma i kapp it-säkerhetsbranscher i tredjeländer bör byrån fastställa och inleda ett långsiktigt unionellt it-säkerhetsprojekt med en räckvidd som är jämförbar med vad som har uppnåtts med Airbus för luftfartsindustrin.

Kommissionens bör i sitt förslag undvika att använda termen ”cybersäkerhet”, eftersom den ur rättslig synvinkel är vag och kan ge upphov till osäkerhet. I stället föreslår föredraganden att man ersätter ”cybersäkerhet” med ”it-säkerhet” för att öka rättssäkerheten.

ÄNDRINGSFÖRSLAG

Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor uppmanar utskottet för industrifrågor, forskning och energi att som ansvarigt utskott beakta följande ändringsförslag:

Ändringsförslag 1

Förslag till förordning
Titel

Kommissionens förslag	*Ändringsförslag*
EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING	EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING
om Enisa, ***”EU:s cybersäkerhetsbyrå”***, och om upphävande av förordning (EU) nr 526/2013, och om ***cybersäkerhetscertifiering*** av informations- och kommunikationsteknik (***”cybersäkerhetsakten”***)	om Enisa, ***den ”europeiska byrån för nät- och informationssäkerhet”***, och om upphävande av förordning (EU) nr 526/2013, och om ***it-säkerhetscertifiering*** av informations- och kommunikationsteknik (***”it-säkerhetsakten”***)
	(Denna ändring berör hela texten.)

Motivering

Prefixet ”cyber”, som härrör från 1960-talets science fiction-verk, har i allt större utsträckning kommit att användas för att beskriva de negativa aspekterna av internet (cyberattack, cyberbrottslighet osv.), men är mycket vagt ur rättslig synvinkel. Föredraganden föreslår en ändring av termen ”cybersäkerhet” till ”it-säkerhet” av rättssäkerhetsskäl.

Ändringsförslag 2

Förslag till förordning
Skäl 2

Kommissionens förslag	*Ändringsförslag*
(2) Användningen av nät- och informationssystem bland allmänheten, företag och regeringar i hela unionen genomsyrar nu hela samhället. Digitalisering och konnektivitet är på väg att bli centrala inslag i ett allt större antal produkter och tjänster, och med tillkomsten av sakernas internet väntas miljoner eller rentav miljarder uppkopplade digitala enheter tas i bruk inom EU under det kommande årtiondet. Trots att allt fler enheter är uppkopplade till internet, är	(2) Användningen av nät- och informationssystem bland allmänheten, företag och regeringar i hela unionen genomsyrar nu hela samhället. Digitalisering och konnektivitet är på väg att bli centrala inslag i ett allt större antal produkter och tjänster, och med tillkomsten av sakernas internet väntas miljoner eller rentav miljarder uppkopplade digitala enheter tas i bruk inom EU under det kommande årtiondet. Trots att allt fler enheter är uppkopplade till internet, är

säkerhet och resiliens inte tillräckligt integrerade i konstruktionen, vilket leder till otillräcklig ***cybersäkerhet***. I detta sammanhang leder den begränsade användningen av certifiering till att organisationer och enskilda användare har otillräcklig information om ***cybersäkerheten*** hos IKT-produkter och IKT-tjänster, vilket undergräver förtroendet för digitala lösningar.

säkerhet och resiliens inte tillräckligt integrerade i konstruktionen, vilket leder till otillräcklig ***it-säkerhet***. I detta sammanhang leder den begränsade ***och fragmenterade*** användningen av certifiering till att organisationer och enskilda användare har otillräcklig information om ***it-säkerheten*** hos IKT-produkter och IKT-tjänster, vilket undergräver förtroendet för digitala lösningar. ***IKT-näten är grundstommen för digitala produkter och tjänster med potential att påverka alla aspekter av medborgarnas liv och påskynda Europas ekonomiska tillväxt. För att säkerställa att målen för den digitala inre marknaden nås helt och hållet måste de väsentliga tekniska byggstenarna som sådana viktiga områden såsom e-hälsa, sakernas internet, artificiell intelligens, kvantteknik samt intelligenta transportsystem och avancerad tillverkning är beroende av finnas på plats.***

Ändringsförslag 3

Förslag till förordning
Skäl 4

Kommissionens förslag	*Ändringsförslag*
(4) Cyberangreppen ökar och en uppkopplad ekonomi och ett uppkopplat samhälle som är mer utsatta för cyberhot och -angrepp kräver starkare skydd. Även om cyberangrepp ofta är gränsöverskridande, är dock de politiska insatserna från ***cybersäkerhetsmyndigheter*** och brottsbekämpande organ till övervägande del nationella. Storskaliga cyberincidenter kan störa tillhandahållandet av grundläggande tjänster i hela EU. Detta kräver en effektiv respons och krishantering på EU-nivå som bygger på särskilt utformade strategier och bredare instrument för europeisk solidaritet och ömsesidigt stöd. För beslutsfattare, näringsliv och användare är det också	(4) Cyberangreppen ökar och en uppkopplad ekonomi och ett uppkopplat samhälle som är mer utsatta för cyberhot och -angrepp kräver starkare ***och säkrare*** skydd. Även om cyberangrepp ofta är gränsöverskridande, är dock de politiska insatserna från ***it-säkerhetsmyndigheter*** och brottsbekämpande organ till övervägande del nationella. Storskaliga cyberincidenter kan störa tillhandahållandet av grundläggande tjänster i hela EU. Detta kräver en effektiv respons och krishantering på EU-nivå som bygger på särskilt utformade strategier och bredare instrument för europeisk solidaritet och ömsesidigt stöd. För beslutsfattare, näringsliv och användare är det också

viktigt att det görs regelbundna bedömningar av situationen när det gäller ***cybersäkerhet*** och resiliens i unionen, på grundval av tillförlitliga unionsdata, samt systematiska prognoser för framtida utveckling, utmaningar och hot på både unionsnivå och global nivå.	viktigt att det görs regelbundna bedömningar av situationen när det gäller ***it-säkerhet*** och resiliens i unionen, på grundval av tillförlitliga unionsdata, samt systematiska prognoser för framtida utveckling, utmaningar och hot på både unionsnivå och global nivå.

Ändringsförslag 4

Förslag till förordning
Skäl 5

Kommissionens förslag	*Ändringsförslag*
(5) Mot bakgrund av de allt större cybersäkerhetsutmaningar som unionen står inför behövs en omfattande uppsättning åtgärder som bygger vidare på tidigare unionsåtgärder och främjar mål som stärker varandra inbördes. Dessa innefattar behovet av att ytterligare öka medlemsstaternas och företagens kapacitet och beredskap samt att förbättra samarbete och samordning mellan medlemsstaterna och EU:s institutioner, byråer och organ. Med tanke på cyberhotens gränsöverskridande karaktär finns det ett behov av att öka kapaciteten på unionsnivå som ett komplement till medlemsstaternas insatser, särskilt när det gäller storskaliga gränsöverskridande cyberincidenter och -kriser. Ytterligare insatser behövs också för att öka allmänhetens och företagens medvetenhet om ***cybersäkerhetsfrågor***. Dessutom bör förtroendet för den digitala inre marknaden stärkas ytterligare genom att transparent information tillhandahålls om säkerhetsnivån för IKT-produkter och IKT-tjänster. Detta kan underlättas genom EU-omfattande certifiering som erbjuder gemensamma ***cybersäkerhetskrav*** och utvärderingskriterier för olika nationella marknader och sektorer.	(5) Mot bakgrund av de allt större cybersäkerhetsutmaningar som unionen står inför behövs en omfattande uppsättning åtgärder som bygger vidare på tidigare unionsåtgärder och främjar mål som stärker varandra inbördes. Dessa innefattar behovet av att ytterligare öka medlemsstaternas och företagens kapacitet och beredskap samt att förbättra samarbete och samordning mellan medlemsstaterna och EU:s institutioner, byråer och organ. Med tanke på cyberhotens gränsöverskridande karaktär finns det ett behov av att öka kapaciteten på unionsnivå som ett komplement till medlemsstaternas insatser, särskilt när det gäller storskaliga gränsöverskridande cyberincidenter och -kriser. Ytterligare insatser behövs också för att ***vidta en samordnad svarsåtgärd på EU-nivå och*** öka allmänhetens och företagens medvetenhet om ***it-säkerhetsfrågor***. Dessutom bör förtroendet för den digitala inre marknaden stärkas ytterligare genom att transparent information tillhandahålls om säkerhetsnivån för IKT-produkter och IKT-tjänster. Detta kan underlättas genom EU-omfattande certifiering som erbjuder gemensamma ***it-säkerhetskrav*** och utvärderingskriterier för olika nationella marknader och sektorer. ***Vid sidan av unionsomfattande certifiering finns en mängd frivilliga åtgärder som är allmänt***

accepterade på marknadsplatsen, beroende på produkt, tjänst, användning eller standard. Dessa åtgärder, samt branschens bottom-up-strategi, inbegripet användning av inbyggd säkerhet, skulduppbyggnad och bidrag till internationella standarder, bör uppmuntras.

Ändringsförslag 5

Förslag till förordning
Skäl 7

Kommissionens förslag	*Ändringsförslag*
(7) Unionen har redan vidtagit viktiga åtgärder för att säkerställa ***cybersäkerhet*** och öka förtroendet för digital teknik. År 2013 antogs EU:s strategi för cybersäkerhet för att vägleda EU:s politiska åtgärder för ***cybersäkerhetshot*** och -risker. I sin satsning för att bättre skydda invånarna på nätet antog unionen 2016 den första rättsakten på området ***cybersäkerhet***, direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan kallat it-säkerhetsdirektivet). It-säkerhetsdirektivet ***införde*** krav om nationell kapacitet på ***cybersäkerhetsområdet***, inrättade de första mekanismerna för att stärka det strategiska och operativa samarbetet mellan medlemsstaterna och införde skyldigheter avseende säkerhetsåtgärder och incidentrapportering inom sektorer som är centrala för ekonomin och samhället, såsom energi, transporter, vatten, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, digital infrastruktur samt leverantörer av viktiga digitala tjänster (sökmotorer, molntjänster och elektroniska marknadsplatser). Enisa fick en viktig roll när det gällde att stödja genomförandet av direktivet. Dessutom är en effektiv kamp	(7) Unionen har redan vidtagit viktiga åtgärder för att säkerställa ***it-säkerhet*** och öka förtroendet för digital teknik. År 2013 antogs EU:s strategi för cybersäkerhet för att vägleda EU:s politiska åtgärder för ***it-säkerhetshot*** och -risker. I sin satsning för att bättre skydda invånarna på nätet antog unionen 2016 den första rättsakten på området ***it-säkerhet***, direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan kallat it-säkerhetsdirektivet). It-säkerhetsdirektivet ***fullbordar strategin för den digitala inre marknaden och inför, tillsammans med andra instrument, såsom direktiv …/… [om inrättandet av en europeisk kodex för elektronisk kommunikation], Europaparlamentets och rådets förordning (EU) 2016/679[1a] och Europaparlamentets och rådets direktiv 2002/58/EG[1b],*** krav om nationell kapacitet på ***it-säkerhetsområdet***, inrättade de första mekanismerna för att stärka det strategiska och operativa samarbetet mellan medlemsstaterna och införde skyldigheter avseende säkerhetsåtgärder och incidentrapportering inom sektorer som är centrala för ekonomin och samhället, såsom energi, transporter, vatten, bankverksamhet, finansmarknadsinfrastruktur, hälso- och

mot it-brottslighet en viktig prioritering i den europeiska säkerhetsagendan, som bidrar till det övergripande målet att uppnå en hög nivå av ***cybersäkerhet***.

sjukvård, digital infrastruktur samt leverantörer av viktiga digitala tjänster (sökmotorer, molntjänster och elektroniska marknadsplatser). Enisa fick en viktig roll när det gällde att stödja genomförandet av direktivet. Dessutom är en effektiv kamp mot it-brottslighet en viktig prioritering i den europeiska säkerhetsagendan, som bidrar till det övergripande målet att uppnå en hög nivå av ***it-säkerhet***.

_____

[1a] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), (EUT L 119, 4.5.2016, s. 1).

[1b] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

Ändringsförslag 6

Förslag till förordning
Skäl 8

Kommissionens förslag	*Ändringsförslag*
(8) Det är allmänt erkänt att den övergripande politiska ramen har förändrats avsevärt sedan antagandet av EU:s strategi för cybersäkerhet 2013 och den senaste översynen av byråns uppdrag, även i förhållande till en mer oviss och mindre säker global miljö. Mot denna bakgrund och inom ramen för unionens nya ***cybersäkerhetsstrategi*** är det nödvändigt att se över Enisas mandat för att definiera dess roll i det förändrade ***cybersäkerhetsekosystemet*** och säkerställa	(8) Det är allmänt erkänt att den övergripande politiska ramen har förändrats avsevärt sedan antagandet av EU:s strategi för cybersäkerhet 2013 och den senaste översynen av byråns uppdrag, även i förhållande till en mer oviss och mindre säker global miljö. Mot denna bakgrund och inom ramen för unionens nya ***it-säkerhetsstrategi*** är det nödvändigt att se över Enisas mandat för att definiera dess roll i det förändrade ***it-säkerhetsekosystemet*** och säkerställa att

att byrån ***bidrar*** effektivt ***till*** unionens reaktion på ***cybersäkerhetsutmaningar*** som härrör från detta radikalt förändrade hotlandskap, för vilket det nuvarande mandatet är inte tillräckligt, vilket också medges i utvärderingen av byrån.	byrån ***tar på sig en ledande roll som på ett*** effektivt ***sätt kommer att förbättra*** unionens reaktion på ***it-säkerhetsutmaningar*** som härrör från detta radikalt förändrade hotlandskap, för vilket det nuvarande mandatet är inte tillräckligt, vilket också medges i utvärderingen av byrån.

Ändringsförslag 7

Förslag till förordning
Skäl 11

Kommissionens förslag	*Ändringsförslag*
(11) Med tanke på de ökande ***cybersäkerhetsutmaningar*** som unionen står inför bör de ekonomiska och personella resurser som anslagits för byrån ökas för att återspegla dess förstärkta roll och arbetsuppgifter och dess centrala position i ekosystemet av organisationer som försvarar det europeiska digitala ekosystemet.	(11) Med tanke på de ökande ***it-säkerhetsutmaningar*** som unionen står inför bör de ekonomiska och personella resurser som anslagits för byrån ökas för att återspegla dess förstärkta roll och arbetsuppgifter och dess centrala position i ekosystemet av organisationer som försvarar det europeiska digitala ekosystemet. ***Ytterligare förstärkning av byråns kapacitet bör beaktas.***

Motivering

Det är av avgörande vikt att vi beaktar byråns bristande kapacitet. Vi måste även sträva mot att fastställa byråns fortsatta utveckling med tanke på hur avgörande it-säkerhet är idag, och än viktigare, hur viktigt det kommer att vara ”i morgon”. Den ryska inblandningen i val måste noteras, samt den ökande kapaciteten hos stormakter och stater runtom i världen och den omedelbart förestående digitaliseringen av stora sektorer.

Ändringsförslag 8

Förslag till förordning
Skäl 11a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(11a) Utmaningarna på it-säkerhetsområdet är, i den digitala tidsåldern, ofta tätt sammanlänkade med utmaningar på området dataskydd,

integritetsskydd samt skydd av elektronisk kommunikation. För att byrån på lämpligt sätt ska kunna ta itu med dessa utmaningar behövs ett nära samarbete och täta samråd med de organ som inrättats genom Europaparlamentets och rådets förordning (EG) 45/2001[1a], förordning (EU) 2016/679, direktiv (EU) 2016/680 och förordning (EG) nr 1211/2009 samt med branschen och det civila samhället.

[1a] 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 (EGT L 8, 12.1.2001, s. 1).

Ändringsförslag 9

Förslag till förordning
Skäl 12

Kommissionens förslag	*Ändringsförslag*
(12) Byrån bör utveckla och upprätthålla en hög nivå av expertis och fungera som en referenspunkt och skapa förtroende och tillit för den inre marknaden genom sin opartiskhet, kvaliteten på de råd och den information den tillhandahåller, öppenheten i dess förfaranden och arbetssätt samt genom ett kompetent utförande av sina uppgifter. Byrån bör aktivt bidra till nationella insatser och unionsinsatser och utföra sina uppgifter i fullt samarbete med unionens institutioner, organ, kontor och byråer samt medlemsstaterna. Byrån bör också stödja sig på synpunkter från och samarbete med den privata sektorn och andra berörda aktörer. ***Genom*** en uppsättning uppgifter ***bör det fastställas hur*** byrån ska uppnå ***sina mål*** samtidigt som flexibilitet i	(12) Byrån bör utveckla och upprätthålla en hög nivå av expertis och fungera som en referenspunkt och skapa förtroende och tillit för den inre marknaden genom sin opartiskhet, kvaliteten på de råd och den information den tillhandahåller, öppenheten i dess förfaranden och arbetssätt samt genom ett kompetent utförande av sina uppgifter. Byrån bör aktivt bidra till nationella insatser och unionsinsatser och utföra sina uppgifter i fullt samarbete med unionens institutioner, organ, kontor och byråer samt medlemsstaterna. Byrån bör också stödja sig på synpunkter från och samarbete med den privata sektorn och andra berörda aktörer. ***En tydlig dagordning och*** en uppsättning uppgifter ***samt mål som*** byrån ska uppnå ***bör definieras tydligt*** samtidigt

verksamheten ***möjliggörs***.	som ***nödvändig*** flexibilitet i verksamheten ***beaktas. Där så är möjligt bör största möjliga insyn och spridning av information upprätthållas.***

Ändringsförslag 10

Förslag till förordning
Skäl 14

Kommissionens förslag	*Ändringsförslag*
(14) ***De*** underliggande uppgiften för byrån är att främja ett konsekvent genomförande av den gällande rättsliga ramen, i synnerhet ett effektivt genomförande av it-säkerhetsdirektivet, vilket är viktigt för att öka cyberresiliensen. Mot bakgrund av det snabbt föränderliga hotlandskapet på ***cybersäkerhetsområdet*** är det uppenbart att medlemsstaterna måste stödjas genom en mer omfattande tvärpolitisk strategi för att bygga upp cyberresiliens.	(14) ***Den*** underliggande uppgiften för byrån är att främja ett konsekvent genomförande av den gällande rättsliga ramen, i synnerhet ett effektivt genomförande av it-säkerhetsdirektivet, ***direktiv …/… [om inrättandet av en europeisk kodex för elektronisk kommunikation], förordning (EU) 2016/679 och direktiv 2002/58/EG,*** vilket är viktigt för att öka cyberresiliensen. Mot bakgrund av det snabbt föränderliga hotlandskapet på ***it-säkerhetsområdet*** är det uppenbart att medlemsstaterna måste stödjas genom en mer omfattande tvärpolitisk strategi för att bygga upp cyberresiliens.

Ändringsförslag 11

Förslag till förordning
Skäl 21a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(21a) Kommissionen bör föreslå obligatoriskt samarbete mellan medlemsstater när det gäller skyddet av kritisk informationsinfrastruktur.

Ändringsförslag 12

Förslag till förordning
Skäl 26

Kommissionens förslag	*Ändringsförslag*
(26) För att bättre förstå utmaningarna inom ***cybersäkerhetsområdet***, och i syfte att tillhandahålla strategisk långsiktig rådgivning till medlemsstaterna och unionens institutioner, behöver byrån analysera nuvarande och framväxande risker. För detta ändamål bör byrån i samarbete med medlemsstaterna och, om lämpligt, med statistikorgan och andra samla in relevant information och utföra analyser av framväxande teknik och tillhandahålla ämnesspecifika bedömningar om förväntade samhälleliga, rättsliga, ekonomiska och regleringsmässiga konsekvenser av tekniska innovationer inom området nät- och informationssäkerhet, i synnerhet ***cybersäkerhet***. Byrån bör också hjälpa medlemsstaterna och unionens institutioner, byråer och organ att identifiera framväxande trender och förebygga problem som rör ***cybersäkerhet***, genom att utföra analyser av hot och ***incidenter***.	(26) För att bättre förstå utmaningarna inom ***it-säkerhetsområdet***, och i syfte att tillhandahålla strategisk långsiktig rådgivning till medlemsstaterna och unionens institutioner, behöver byrån analysera nuvarande och framväxande risker***, incidenter och sårbarheter***. För detta ändamål bör byrån i samarbete med medlemsstaterna och, om lämpligt, med statistikorgan och andra samla in relevant information och utföra analyser av framväxande teknik och tillhandahålla ämnesspecifika bedömningar om förväntade samhälleliga, rättsliga, ekonomiska och regleringsmässiga konsekvenser av tekniska innovationer inom området nät- och informationssäkerhet, i synnerhet ***it-säkerhet***. Byrån bör också hjälpa medlemsstaterna och unionens institutioner, byråer och organ att identifiera framväxande trender och förebygga problem som rör ***it-säkerhet***, genom att utföra analyser av hot***,*** ***incidenter*** och ***sårbarheter***.

Ändringsförslag 13

Förslag till förordning
Skäl 28

Kommissionens förslag	*Ändringsförslag*
(28) Byrån bör bidra till att öka allmänhetens medvetenhet om ***cybersäkerhetsrisker*** och ge vägledning om god praxis för enskilda användare riktad till privatpersoner och organisationer. ***Byrån*** bör även bidra till att främja bästa praxis och lösningar för enskilda och organisationer genom att samla in och analysera offentligt tillgänglig information om betydande incidenter och genom att sammanställa rapporter i syfte att ge vägledning till företag ***och*** privatpersoner och ***att höja den allmänna***	(28) Byrån bör bidra till att öka allmänhetens medvetenhet om ***it-säkerhetsrisker*** och ge vägledning om god praxis för enskilda användare riktad till privatpersoner och organisationer. ***För att höja den allmänna beredskaps- och resiliensnivån*** bör ***byrån*** även bidra till att främja bästa praxis och lösningar för enskilda och organisationer genom att samla in och analysera offentligt tillgänglig information om betydande incidenter och genom att sammanställa rapporter i syfte att ge vägledning till företag***,***

beredskaps- och resiliensnivån. Byrån bör vidare, i samarbete med medlemsstaterna och unionens institutioner, organ, kontor och byråer, organisera informations- och folkbildningskampanjer riktade till slutanvändare***, i syfte att*** främja ett säkrare beteende bland enskilda internetanvändare och höja medvetenheten om de potentiella hoten i cyberrymden, bland annat it-brottslighet såsom phishingattacker, botnät, ekonomiska bedrägerier och bankbedrägerier, samt ***främja*** grundläggande ***rådgivning om autentisering*** och ***dataskydd***. Byrån bör spela en central roll när det gäller att höja slutanvändarnas medvetenhet om enheters säkerhet.

privatpersoner och ***relevanta myndigheter på unionsnivå och på nationell nivå***. Byrån bör vidare, i samarbete med medlemsstaterna och unionens institutioner, organ, kontor och byråer, organisera informations- och folkbildningskampanjer riktade till slutanvändare***. Dessa kampanjer bör*** främja ***utbildning i it-säkerhet och*** ett säkrare beteende bland enskilda internetanvändare och höja medvetenheten om de potentiella hoten i cyberrymden, bland annat it-brottslighet såsom phishingattacker, botnät, ekonomiska bedrägerier och bankbedrägerier, ***förfalskning och olagligt innehåll,*** samt ***förespråka dataskydd och*** grundläggande ***autentisering för att förhindra stöld av data*** och ***identiteter***. Byrån bör spela en central roll när det gäller att höja slutanvändarnas medvetenhet om enheters säkerhet.

Ändringsförslag 14

Förslag till förordning
Skäl 28a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(28a) Byrån bör höja allmänhetens medvetenhet om riskerna med incidenter rörande databedrägeri och datastöld som kan få allvarliga konsekvenser för enskildas grundläggande rättigheter, utgöra ett hot mot rättsstatsprincipen och riskera stabiliteten i demokratiska samhällen, inbegripet de demokratiska processerna i medlemsstaterna.

Ändringsförslag 15

Förslag till förordning
Skäl 30

Kommissionens förslag	*Ändringsförslag*

(30) För att se till att byrån fullt ut uppnår sina mål bör den samarbeta med berörda institutioner, byråer och organ, däribland CERT-EU, Europeiska it-brottscentrumet (EC3) vid Europol, Europeiska försvarsbyrån (EDA), Europeiska byrån för den operativa förvaltningen av stora it-system (eu-LISA), Europeiska byrån för luftfartssäkerhet (Easa) och andra EU-organ som arbetar med ***cybersäkerhet***. Byrån bör också samverka med myndigheter som hanterar dataskydd för att utbyta sakkunskap och bästa praxis samt ge råd om ***cybersäkerhetsaspekter*** som kan påverka deras arbete. Företrädare för medlemsstaternas och unionens rättsvårdande myndigheter och dataskyddsmyndigheter bör ha rätt att företrädas i byråns ständiga intressentgrupp. I samarbetet med rättsvårdande organ om nät- och informationssäkerhetsaspekter som kan påverka deras arbete bör byrån använda existerande informationskanaler och etablerade nätverk.	(30) För att se till att byrån fullt ut uppnår sina mål bör den samarbeta med berörda institutioner, byråer och organ, däribland CERT-EU, Europeiska it-brottscentrumet (EC3) vid Europol, Europeiska försvarsbyrån (EDA), Europeiska byrån för den operativa förvaltningen av stora it-system (eu-LISA), Europeiska byrån för luftfartssäkerhet (Easa)***, Europeiska byrån för GNSS (GSA)*** och andra EU-organ som arbetar med ***it-säkerhet***. Byrån bör också samverka med ***unionella och nationella*** myndigheter som hanterar dataskydd för att utbyta sakkunskap och bästa praxis samt ge råd om ***it-säkerhetsaspekter*** som kan påverka deras arbete. Företrädare för medlemsstaternas och unionens rättsvårdande myndigheter och dataskyddsmyndigheter bör ha rätt att företrädas i byråns ständiga intressentgrupp. I samarbetet med rättsvårdande organ om nät- och informationssäkerhetsaspekter som kan påverka deras arbete bör byrån använda existerande informationskanaler och etablerade nätverk.

Motivering

Eftersom det finns it-säkerhetsproblem inom Galileo, särskilt inom jordsegmenten, stärker faktiskt samarbetet med Europeiska byrån för GNSS Enisas roll samtidigt som det ökar Galileos trovärdighet.

Ändringsförslag 16

Förslag till förordning
Skäl 35

Kommissionens förslag	*Ändringsförslag*
(35) Byrån bör uppmuntra medlemsstaterna och ***tjänsteleverantörerna*** att höja sina allmänna säkerhetsstandarder så att alla internetanvändare kan vidta de åtgärder som krävs för att trygga sin egen	(35) Byrån bör uppmuntra medlemsstaterna***, maskinvaru-*** och ***programvarutillverkarna samt IKT- och onlinetjänsteleverantörerna*** att höja sina allmänna säkerhetsstandarder så att alla internetanvändare kan vidta de åtgärder

cybersäkerhet. I synnerhet bör tjänsteleverantörer och produkttillverkare återkalla eller återvinna produkter och tjänster som inte uppfyller ***cybersäkerhetsstandarderna***. I samarbete med de behöriga myndigheterna kan Enisa sprida uppgifter om ***cybersäkerhetsnivån*** för de produkter och tjänster som erbjuds på den inre marknaden, och utfärda varningar riktade till leverantörer och tillverkare och ålägga dem att förbättra sina produkters och tjänsters säkerhet, inbegripet ***cybersäkerhet***.

som krävs för att trygga sin egen ***it-säkerhet***. I synnerhet bör tjänsteleverantörer och produkttillverkare återkalla eller återvinna produkter och tjänster som inte uppfyller ***it-säkerhetsstandarderna***. I samarbete med de behöriga myndigheterna kan Enisa sprida uppgifter om ***it-säkerhetsnivån*** för de produkter och tjänster som erbjuds på den inre marknaden, och utfärda varningar riktade till leverantörer och tillverkare och ålägga dem att förbättra sina produkters och tjänsters säkerhet, inbegripet ***it-säkerhet. Byrån bör samarbeta med intressenter för att utarbeta en unionsomfattande strategi för ett ansvarsfullt utlämnande av uppgifter om sårbarheter, och bör främja bästa praxis på detta område.***

Ändringsförslag 17

Förslag till förordning
Skäl 44

Kommissionens förslag	*Ändringsförslag*
(44) Byrån bör ha en ständig intressentgrupp som rådgivande organ, för att säkerställa en regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda intressenter. Den ständiga intressentgruppen, som inrättas av styrelsen på förslag av den verkställande direktören, bör koncentrera sig på frågor som är relevanta för intressenter och uppmärksamma byrån på dem. Den ständiga intressentgruppens sammansättning och de uppgifter som anförtrotts denna grupp, som särskilt rådfrågas om utkastet till arbetsprogram, bör säkerställa en tillräcklig representation av intressenter i byråns arbete.	(44) Byrån bör ha en ständig intressentgrupp som rådgivande organ, för att säkerställa en regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda intressenter. Den ständiga intressentgruppen, som inrättas av styrelsen på förslag av den verkställande direktören, bör koncentrera sig på frågor som är relevanta för intressenter och uppmärksamma byrån på dem. Den ständiga intressentgruppens sammansättning och de uppgifter som anförtrotts denna grupp, som särskilt rådfrågas om utkastet till arbetsprogram, bör säkerställa en tillräcklig representation av intressenter i byråns arbete. ***Med tanke på vikten av certifieringskrav för att säkerställa förtroende för sakernas internet bör kommissionen särskilt beakta genomförandeåtgärder för att säkerställa***

	unionsomfattande harmonisering av säkerhetsstandarder för sakernas internet.

Ändringsförslag 18

Förslag till förordning
Skäl 50

Kommissionens förslag	*Ändringsförslag*
(50) För närvarande används ***cybersäkerhetscertifiering*** av IKT-produkter och IKT-tjänster endast i begränsad omfattning. I de fall det förekommer är det oftast på medlemsstatsnivå eller inom ramen för industridrivna system. Ett certifikat utfärdat av en nationell ***cybersäkerhetsmyndighet*** i ett sådant sammanhang erkänns i princip inte av andra medlemsstater. Företag kan därför behöva certifiera sina produkter och tjänster i flera medlemsstater där de bedriver verksamhet, exempelvis för att kunna delta i nationella upphandlingsförfaranden. Även om nya system utvecklas, tycks det inte finnas någon samlad helhetssyn på övergripande ***cybersäkerhetsfrågor***, exempelvis inom området sakernas internet. Befintliga system uppvisar allvarliga brister och skillnader i fråga om produkttäckning, assuransnivå, grundläggande kriterier och faktisk användning.	(50) För närvarande används ***it-säkerhetscertifiering*** av IKT-produkter och IKT-tjänster endast i begränsad omfattning. I de fall det förekommer är det oftast på medlemsstatsnivå eller inom ramen för industridrivna system. Ett certifikat utfärdat av en nationell ***it-säkerhetsmyndighet*** i ett sådant sammanhang erkänns i princip inte av andra medlemsstater. Företag kan därför behöva certifiera sina produkter och tjänster i flera medlemsstater där de bedriver verksamhet, exempelvis för att kunna delta i nationella upphandlingsförfaranden***, och dessa förfaranden kan medföra extra kostnader för företagen***. Även om nya system utvecklas, tycks det inte finnas någon samlad helhetssyn på övergripande ***it-säkerhetsfrågor***, exempelvis inom området sakernas internet. Befintliga system uppvisar allvarliga brister och skillnader i fråga om produkttäckning, assuransnivå, grundläggande kriterier och faktisk användning. ***I syfte att säkerställa att tjänster och produkter omfattas av lämpliga certifieringssystem bör en bedömning från fall till fall ske. Därtill tarvas en riskbaserad strategi för en effektiv identifiering av risker och riskreducering och för att undvika ökade kostnader för tillverkarna.***

Ändringsförslag 19

Förslag till förordning
Skäl 52

Kommissionens förslag	*Ändringsförslag*
(52) Mot bakgrund av ovanstående är det nödvändigt att inrätta en europeisk ram för ***cybersäkerhetscertifiering*** som fastställer de viktigaste övergripande kraven för europeiska system för ***cybersäkerhetscertifiering*** som ska utvecklas, och som gör att certifikat för IKT-produkter och IKT-tjänster kan erkännas och användas i samtliga medlemsstater. Den europeiska ramen bör ha ett dubbelt syfte: Å ena sidan bör den bidra till att öka förtroendet för IKT-produkter och IKT-tjänster som har certifierats enligt sådana system. Å andra sidan bör den undvika att det uppstår flera olika motstridiga eller överlappande nationella ***cybersäkerhetscertifieringar*** och därmed minska kostnaderna för företag som är verksamma på den digitala inre marknaden. Systemen bör vara icke-diskriminerande och grundas på internationella och/eller unionens standarder såvida inte dessa standarder är ineffektiva eller olämpliga för att förverkliga EU:s legitima mål i detta avseende.	(52) Mot bakgrund av ovanstående är det nödvändigt att inrätta en ***harmoniserad*** europeisk ram för ***it-säkerhetscertifiering*** som fastställer de viktigaste övergripande kraven för europeiska system för ***it-säkerhetscertifiering*** som ska utvecklas, och som gör att certifikat för IKT-produkter och IKT-tjänster kan erkännas och användas i samtliga medlemsstater. Den europeiska ramen bör ha ett dubbelt syfte: Å ena sidan bör den bidra till att öka förtroendet för IKT-produkter och IKT-tjänster som har certifierats enligt sådana system. Å andra sidan bör den undvika att det uppstår flera olika motstridiga eller överlappande nationella ***it-säkerhetscertifieringar*** och därmed minska kostnaderna för företag som är verksamma på den digitala inre marknaden. Systemen bör vara icke-diskriminerande och grundas på internationella och/eller unionens standarder såvida inte dessa standarder är ineffektiva eller olämpliga för att förverkliga EU:s legitima mål i detta avseende.

Ändringsförslag 20

Förslag till förordning
Skäl 55

Kommissionens förslag	*Ändringsförslag*
(55) Syftet med europeiska system för ***cybersäkerhetscertifiering*** bör vara att se till att IKT-produkter och IKT-tjänster som certifierats enligt ett sådant system uppfyller de angivna kraven. Dessa krav gäller förmågan att, vid en viss assuransnivå, stå emot åtgärder som syftar till att äventyra tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller	(55) Syftet med europeiska system för ***it-säkerhetscertifiering*** bör vara att se till att IKT-produkter och IKT-tjänster som certifierats enligt ett sådant system uppfyller de angivna kraven. Dessa krav gäller förmågan att, vid en viss assuransnivå, stå emot åtgärder som syftar till att äventyra tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller

de därmed sammanhängande funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, processer, tjänster och system i den mening som avses i denna förordning. Det är inte möjligt att i denna förordning i detalj fastställa ***cybersäkerhetskraven*** för alla IKT-produkter och IKT-tjänster. IKT-produkter och IKT-tjänster och relaterade ***cybersäkerhetsbehov*** är så olikartade att det är mycket svårt att ta fram allmänna ***cybersäkerhetskrav*** som är giltiga över hela linjen. Det är därför nödvändigt att anta ett brett och allmänt ***cybersäkerhetsbegrepp*** när det gäller certifieringsändamål, kompletterat med en uppsättning specifika ***cybersäkerhetmål*** som måste beaktas vid utformningen av europeiska system för ***cybersäkerhetscertifiering***. Formerna för att uppnå dessa mål i specifika IKT-produkter och IKT-tjänster bör sedan fastställas i detalj för det enskilda certifieringssystem som antas av kommissionen, till exempel genom hänvisningar till standarder eller tekniska specifikationer.	de därmed sammanhängande funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, processer, tjänster och system i den mening som avses i denna förordning. Det är inte möjligt att i denna förordning i detalj fastställa ***it-säkerhetskraven*** för alla IKT-produkter och IKT-tjänster. IKT-produkter och IKT-tjänster och relaterade ***it-säkerhetsbehov*** är så olikartade***, och detsamma gäller dessas livscykel,*** att det är mycket svårt att ta fram allmänna ***it-säkerhetskrav*** som är giltiga över hela linjen. Det är därför nödvändigt att anta ett brett och allmänt ***it-säkerhetsbegrepp*** när det gäller certifieringsändamål, kompletterat med en uppsättning specifika ***it-säkerhetmål*** som måste beaktas vid utformningen av europeiska system för ***it-säkerhetscertifiering***. Formerna för att uppnå dessa mål i specifika IKT-produkter och IKT-tjänster bör sedan fastställas i detalj för det enskilda certifieringssystem som antas av kommissionen ***i nära samråd med medlemsstaterna och industriaktörer***, till exempel genom hänvisningar till standarder eller tekniska specifikationer. ***De enskilda certifieringssystemen bör utformas på ett sådant sätt att alla aktörer som deltar i utvecklingen av relevanta it-produkter och it-tjänster uppmanas att utarbeta och anta standarder, normer och principer som säkerställer högsta möjliga säkerhetsnivå under hela livscykeln.***

Ändringsförslag 21

Förslag till förordning
Skäl 55a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(55a) Enisa bör utarbeta ett certifieringssystem med ett globalt perspektiv i syfte att förhindra framtida handelshinder. Vid utarbetandet av kriterierna för certifieringssystemet bör Enisa föra en dialog med relevanta

partner i sektorn för att säkerställa den kommersiella genomförbarheten.

Ändringsförslag 22

Förslag till förordning
Skäl 56

Kommissionens förslag	*Ändringsförslag*
(56) Kommissionen bör ges befogenhet att begära att Enisa förbereder förslag till system för särskilda IKT-produkter eller IKT-tjänster. Kommissionen bör, på grundval av Enisas förslag till system, ges befogenhet att anta det europeiska ***certifieringssystemet*** genom genomförandeakter. Med beaktande av det allmänna syfte och de säkerhetsmål som fastställs i denna förordning bör det i europeiska ***certifieringssystem*** som antas av kommissionen specificeras en minimiuppsättning komponenter avseende det enskilda systemets föremål, tillämpningsområde och funktionssätt. Dessa bör bland annat omfatta ***cybersäkerhetscertifieringens*** tillämpningsområde och föremål, inklusive de kategorier av IKT-produkter och IKT-tjänster som omfattas, den detaljerade specifikationen av ***cybersäkerhetskraven***, exempelvis genom hänvisning till standarder eller tekniska specifikationer, de särskilda utvärderingskriterierna och utvärderingsmetoderna samt den avsedda assuransnivån: grundläggande, betydande och/eller hög.	(56) Kommissionen bör ges befogenhet att begära att Enisa förbereder förslag till system för särskilda IKT-produkter eller IKT-tjänster. Kommissionen bör, på grundval av Enisas förslag till system, ges befogenhet att anta det europeiska ***it-certifieringssystemet*** genom genomförandeakter. Med beaktande av det allmänna syfte och de säkerhetsmål som fastställs i denna förordning bör det i europeiska ***it-certifieringssystem*** som antas av kommissionen specificeras en minimiuppsättning komponenter avseende det enskilda systemets föremål, tillämpningsområde och funktionssätt. Dessa bör bland annat omfatta ***it-säkerhetscertifieringens*** tillämpningsområde och föremål, inklusive de kategorier av IKT-produkter och IKT-tjänster som omfattas, den detaljerade specifikationen av ***it-säkerhetskraven***, exempelvis genom hänvisning till standarder eller tekniska specifikationer, de särskilda utvärderingskriterierna och utvärderingsmetoderna samt den avsedda assuransnivån: grundläggande, betydande och/eller hög. ***Assuransnivåerna bör fastställas från fall till fall för att säkerställa att IKT-tjänsterna och IKT-produkterna omfattas av lämpliga certifieringssystem. De bör även beakta de olika enskilda användningsområdena samt användarnas eget ansvar och utbildning.***

Ändringsförslag 23

Förslag till förordning
Skäl 57

Kommissionens förslag	*Ändringsförslag*
(57) Användningen av europeisk ***cybersäkerhetscertifiering*** bör vara frivillig, om inte annat föreskrivs i unionslagstiftning eller nationell lagstiftning. I syfte att uppnå målen för denna förordning och undvika en fragmentering av den inre marknaden, bör dock nationella system eller förfaranden för ***cybersäkerhetscertifiering*** av IKT-produkter och IKT-tjänster som omfattas av ett europeiskt system för ***cybersäkerhetscertifiering*** upphöra att ha verkan från och med den dag som fastställs av kommissionen genom en genomförandeakt. Vidare bör medlemsstaterna inte införa nya nationella certifieringssystem som tillhandahåller ***cybersäkerhetscertifiering*** av IKT-produkter och IKT-tjänster som redan omfattas av ett befintligt europeiskt system för ***cybersäkerhetscertifiering***.	(57) Användningen av europeisk ***it-säkerhetscertifiering*** bör vara frivillig, om inte annat föreskrivs i unionslagstiftning eller nationell lagstiftning. ***Efter detta inledande skede, och beroende av hur långt genomförandet har framskridit i medlemsstaterna och av en produkts eller tjänsts avgörande betydelse, kan potentiellt obligatoriska system för vissa IKT-produkter och IKT-tjänster i framtiden komma att införas inom ramen för en strategi som är indelad i faser för framtida teknikgenerationer och som svar på morgondagens politiska mål.*** I syfte att uppnå målen för denna förordning och undvika en fragmentering av den inre marknaden, bör dock nationella system eller förfaranden för ***it-säkerhetscertifiering*** av IKT-produkter och IKT-tjänster som omfattas av ett europeiskt system för ***it-säkerhetscertifiering*** upphöra att ha verkan från och med den dag som fastställs av kommissionen genom en genomförandeakt. Vidare bör medlemsstaterna inte införa nya nationella certifieringssystem som tillhandahåller ***it-säkerhetscertifiering*** av IKT-produkter och IKT-tjänster som redan omfattas av ett befintligt europeiskt system för ***it-säkerhetscertifiering***.

Ändringsförslag 24

Förslag till förordning
Skäl 58a (nytt)

Kommissionens förslag	*Ändringsförslag*
	(58a) Tydliga grundläggande it-säkerhetskrav bör utformas av byrån och läggas fram för kommissionen som genomförandeakter, om så är tillämpligt,

	för alla it-enheter som säljs i eller exporteras från unionen. Dessa krav bör ses över vartannat år därefter, för att säkerställa kontinuerlig förbättring. Dessa grundläggande it-säkerhetskrav bör bland annat medföra att enheterna inte innehåller några kända säkerhetsbrister som kan utnyttjas, att de har kapacitet att godta betrodda säkerhetsuppdateringar, att försäljaren meddelar behöriga myndigheter om kända brister och reparationer eller ersätter berörda enheter fram till den tidpunkt då försäljaren har tydliggjort att säkerhetssupporten för sådana enheter upphör.

Ändringsförslag 25

Förslag till förordning
Artikel 1 – led b

Kommissionens förslag	*Ändringsförslag*
(b) fastställa en ram för inrättandet av europeiska system för ***cybersäkerhetscertifiering*** i syfte att säkerställa en tillfredsställande nivå i fråga om ***cybersäkerhet*** för IKT-produkter och IKT-tjänster i unionen. En sådan ram ska användas utan att det påverkar tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsakter.	(b) fastställa en ram för inrättandet av europeiska system för ***it-säkerhetscertifiering*** i syfte att säkerställa en tillfredsställande nivå i fråga om ***it-säkerhet*** för IKT-produkter och IKT-tjänster i unionen. En sådan ram ska användas utan att det påverkar tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsakter.

Motivering

En rent språklig ändring som stryker den pleonasm som finns i kommissionens text.

Ändringsförslag 26

Förslag till förordning
Artikel 2 – led 8

Kommissionens förslag	*Ändringsförslag*
(8) cyberhot: en potentiell	(8) cyberhot: en potentiell

omständighet eller händelse som på ett negativt sätt kan påverka nät- och informationssystem, deras användare och berörda personer.	omständighet***, kapacitet*** eller händelse som på ett negativt sätt kan påverka nät- och informationssystem, deras användare och berörda personer.

Motivering

Lägger till en viktig aspekt, i synnerhet vad gäller hotbedömning.

Ändringsförslag 27

Förslag till förordning
Artikel 4 – punkt 3 – stycke 1a (nytt)

Kommissionens förslag	*Ändringsförslag*
	Byrån ska försöka fastställa kritiska sårbarheter inom unionens it-säkerhetsnät i dess helhet, samt sådana hos enskilda medlemsstater. Om byrån anser det vara nödvändigt bör sådana sårbarheter rapporteras till Europaparlamentet.

Ändringsförslag 28

Förslag till förordning
Artikel 4 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. Byrån ska öka ***cybersäkerhetskapaciteten*** på unionsnivå i syfte att komplettera medlemsstaternas åtgärder för att förebygga och vidta åtgärder mot cyberhot, särskilt vid gränsöverskridande incidenter.	5. Byrån ska öka ***it-säkerhetskapaciteten*** på unionsnivå i syfte att komplettera ***och stödja*** medlemsstaternas åtgärder för att förebygga och vidta åtgärder mot cyberhot, särskilt vid gränsöverskridande incidenter.

Ändringsförslag 29

Förslag till förordning
Artikel 4 – punkt 6

Kommissionens förslag	*Ändringsförslag*

6. Byrån ska främja användningen av certifiering, bland annat genom att bidra till inrättandet och upprätthållandet av en ram för ***cybersäkerhetscertifiering*** på unionsnivå i enlighet med avdelning III i denna förordning, i syfte att öka transparensen i fråga om assuransnivån för ***cybersäkerhet*** hos IKT-produkter och IKT-tjänster och därigenom stärka förtroendet för den digitala inre marknaden.	6. Byrån ska främja användningen av certifiering, bland annat genom att bidra till ***utvecklingen av unionella och internationella standarder för it-säkerhet,*** inrättandet och upprätthållandet av en ram för ***it-säkerhetscertifiering*** på unionsnivå i enlighet med avdelning III i denna förordning, i syfte att öka transparensen i fråga om assuransnivån för ***it-säkerhet*** hos IKT-produkter och IKT-tjänster och därigenom stärka förtroendet för den digitala inre marknaden.

Ändringsförslag 30

Förslag till förordning
Artikel 4 – punkt 7

Kommissionens förslag	*Ändringsförslag*
7. Byrån ska främja en hög medvetenhet ***hos allmänheten och företagen*** i frågor som rör ***cybersäkerhet***.	7. Byrån ska främja en hög medvetenhet i frågor som rör ***it-säkerhet***.

Motivering

Medvetenhet bör inte endast främjas hos allmänheten och företagen, utan hos alla relevanta aktörer i samhället, inbegripet myndigheter och lagstiftare. Detta ändringsförslag lämnar avsiktligen öppet vilka denna typ av verksamhet ska rikta sig mot.

Ändringsförslag 31

Förslag till förordning
Artikel 5 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. hjälpa medlemsstaterna att på ett konsekvent sätt genomföra unionens politik och lagstiftning som rör ***cybersäkerhet***, i synnerhet vad gäller direktiv (EU) 2016/1148, bland annat genom yttranden, riktlinjer, råd och bästa praxis i frågor såsom riskhantering, incidentrapportering och	2. hjälpa medlemsstaterna att på ett konsekvent sätt genomföra unionens politik och lagstiftning som rör ***it-säkerhet***, i synnerhet vad gäller direktiv (EU) 2016/1148***, direktiv …/… [om inrättandet av en europeisk kodex för elektronisk kommunikation], förordning (EU) 2016/679 och direktiv 2002/58/EG***, bland

informationsutbyte, samt underlätta utbytet av bästa praxis mellan behöriga myndigheter i detta avseende,	annat genom yttranden, riktlinjer, råd och bästa praxis i frågor såsom riskhantering, incidentrapportering och informationsutbyte, samt underlätta utbytet av bästa praxis mellan behöriga myndigheter i detta avseende,

Ändringsförslag 32

Förslag till förordning
Artikel 5 – punkt 2a (ny)

Kommissionens förslag	*Ändringsförslag*
	2a. hjälpa Europeiska dataskyddsstyrelsen, som inrättades genom förordning (EU) 2016/679, att utarbeta riktlinjer för att på teknisk nivå specificera villkoren som möjliggör för registeransvariga att lagligen använda personuppgifter för it-säkerhetsändamål i syfte att skydda deras infrastruktur genom att upptäcka och stoppa attacker mot deras informationssystem inom ramen för följande:
	(i) förordning (EU) 2016/679,
	(ii) direktiv (EU) 2016/1148 och
	(iii) Direktiv 2002/58/EG.

Ändringsförslag 33

Förslag till förordning
Artikel 5 – punkt 2b (ny)

Kommissionens förslag	*Ändringsförslag*
	2b. föreslå riktlinjer för att se till att IKT-försäljare agerar med tillbörlig aktsamhet när det gäller att i tid åtgärda brister i it-säkerheten i deras produkter och tjänster för att undvika att i onödan utsätta användare för it-brottslighet,

Ändringsförslag 34

Förslag till förordning
Artikel 5 – punkt 2c (ny)

Kommissionens förslag	*Ändringsförslag*
	2c. föreslå riktlinjer som inrättar en stark känsla av ansvarsskyldighet för samtliga intressenter (inbegripet slutanvändare) som deltar IKT-ekosystem,

Ändringsförslag 35

Förslag till förordning
Artikel 5 – punkt 2d (ny)

Kommissionens förslag	*Ändringsförslag*
	2d. föreslå riktlinjer i enlighet med nationell lagstiftning rörande skyldigheter för operatörer av viktig nätinfrastruktur vid angrepp mot deras informationssystem som påverkar deras användare till följd av brist på tillbörlig aktsamhet från vissa användare eller operatören själv, där operatören har underlåtit att vidta rimliga åtgärder för att förhindra incidenten eller mildra dess effekter för alla användare,

Ändringsförslag 36

Förslag till förordning
Artikel 5 – punkt 2e (ny)

Kommissionens förslag	*Ändringsförslag*
	2e. föreslå riktlinjer för att begränsa offentliga myndigheters förvärvande och bruk av ”Zero days” i syfte att angripa informationssystem samt främja programvaruutvärdering och finansiera sakkunnig personal,

Ändringsförslag 37

Förslag till förordning
Artikel 5 – punkt 2f (ny)

Kommissionens förslag	*Ändringsförslag*
	2f. föreslå riktlinjer för offentliga myndigheter, privata företag, forskare, universitet och andra intressenter att offentliggöra alla kritiska säkerhetsbrister som ännu inte är allmänt kända inom ramen för ett ansvarsfullt utlämnande av uppgifter,

Ändringsförslag 38

Förslag till förordning
Artikel 5 – punkt 2g (ny)

Kommissionens förslag	*Ändringsförslag*
	2g. föreslå riktlinjer för en bredare användning av ”kontrollerbar öppen källkod” för it-lösningar inom den offentliga sektorn samt för den närliggande användningen av automatiserade verktyg för att underlätta översynen av källkod och för att lätt kunna verifiera frånvaron av bakdörrar och andra eventuella säkerhetsbrister,

Ändringsförslag 39

Förslag till förordning
Artikel 6 – punkt 1 – led fa (nytt)

Kommissionens förslag	*Ändringsförslag*
	(fa) och samarbeta med nationella tillsynsmyndigheter för dataskydd, där så krävs,

Ändringsförslag 40

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

Kommissionens förslag	*Ändringsförslag*
	2a. Byrån ska underlätta inrättandet och lanserandet av ett långsiktigt europeiskt it-säkerhetsprojekt till stöd för tillväxten av en oberoende it-säkerhetsindustri i EU, samt integrera it-säkerheten i all it-utveckling inom EU.

Motivering

Enisa bör bistå lagstiftarna när det gäller utarbetandet av en politik som gör det möjligt för EU att komma i kapp it-säkerhetsindustrier i tredjeland. Projektet bör vara jämförbart i omfattning till vad som tidigare har uppnåtts inom flygbranschen (se exemplet Airbus). Detta behövs för att utveckla en starkare, självständig och pålitlig IKT-industri i EU (se enheten för vetenskaplig framsyn (Stoa), studie PE 614.531).

Ändringsförslag 41

Förslag till förordning
Artikel 7 – punkt 5

Kommissionens förslag	*Ändringsförslag*
5. På begäran av ***två eller flera berörda medlemsstater***, och med det enda syftet att tillhandahålla råd för att förebygga framtida incidenter, ska byrån stödja eller genomföra en teknisk efterhandsundersökning som svar på rapporter från berörda företag om incidenter som har en betydande eller avsevärd inverkan enligt direktiv (EU) 2016/1148. Byrån ska också genomföra en sådan undersökning efter en vederbörligen motiverad begäran från kommissionen, i samförstånd med de berörda medlemsstaterna, om sådana incidenter berör fler än två medlemsstater.	5. På begäran av ***en medlemsstat***, och med det enda syftet att tillhandahålla råd för att förebygga framtida incidenter, ska byrån stödja eller genomföra en teknisk efterhandsundersökning som svar på rapporter från berörda företag om incidenter som har en betydande eller avsevärd inverkan enligt direktiv (EU) 2016/1148. Byrån ska också genomföra en sådan undersökning efter en vederbörligen motiverad begäran från kommissionen, i samförstånd med de berörda medlemsstaterna, om sådana incidenter berör fler än två medlemsstater.
Omfattningen av undersökningen och det förfarande som ska följas vid	Omfattningen av undersökningen och det förfarande som ska följas vid

genomförandet av en sådan undersökning, ska överenskommas av de berörda medlemsstaterna och byrån och ska inte påverka eventuella pågående brottsutredningar om samma incident. Undersökningen ska avslutas med en slutlig teknisk rapport som sammanställs av byrån, i synnerhet på grundval av information och synpunkter från de berörda medlemsstaterna och företagen, och fastställs tillsammans med de berörda medlemsstaterna. En sammanfattning av rapporten, med fokusering på rekommendationer för att förebygga framtida incidenter, kommer att distribueras till CSIRT-nätverket.	genomförandet av en sådan undersökning, ska överenskommas av de berörda medlemsstaterna och byrån och ska inte påverka eventuella pågående brottsutredningar om samma incident ***eller medlemsstaters nationella säkerhetsåtgärder***. Undersökningen ska avslutas med en slutlig teknisk rapport som sammanställs av byrån, i synnerhet på grundval av information och synpunkter från de berörda medlemsstaterna och företagen, och fastställs tillsammans med de berörda medlemsstaterna. En sammanfattning av rapporten, med fokusering på rekommendationer för att förebygga framtida incidenter, kommer att distribueras till CSIRT-nätverket.

Ändringsförslag 42

Förslag till förordning
Artikel 7 – punkt 8a (ny)

Kommissionens förslag	*Ändringsförslag*
	8a. Byrån ska, på begäran av unionens institutioner, organ, kontor eller byråer, eller av en medlemsstat, genomföra regelbundna oberoende it-säkerhetsgranskningar av kritiska infrastrukturer i syfte att identifiera eventuella rekommendationer för att stärka deras motståndskraft.

Motivering

Enisa bör ges befogenhet att genomföra förebyggande it-säkerhetsgranskning av kritisk infrastruktur som drivs av medlemsstaternas myndigheter eller EU:s institutioner, byråer m.fl.

Ändringsförslag 43

Förslag till förordning
Artikel 8 – led a – led 1

Kommissionens förslag	*Ändringsförslag*
(1) utarbeta förslag till europeiska system för ***cybersäkerhetscertifiering*** för IKT-produkter och IKT-tjänster i enlighet med artikel 44 i denna förordning,	(1) utarbeta förslag till europeiska system för ***it-säkerhetscertifiering*** för IKT-produkter och IKT-tjänster i ***samarbete med branschen och i*** enlighet med artikel 44 i denna förordning,

Motivering

På detta område är branschsamarbete viktigt.

Ändringsförslag 44

Förslag till förordning
Artikel 8 – led ca (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ca) införa certifieringssystem som hindrar IKT-försäljare och andra tjänsteleverantörer att introducera hemliga bakdörrar som avsiktligt försämrar it-säkerheten i kommersiella produkter och tjänster och har en negativ inverkan på den globala säkerheten på internet,

Motivering

Detta bör erkännas som ett av huvudmålen för certifieringssystemen.

Ändringsförslag 45

Förslag till förordning
Artikel 9 – led d

Kommissionens förslag	*Ändringsförslag*
(d) via en särskild portal samla, organisera och för allmänheten tillgängliggöra information om ***cybersäkerhet*** som tillhandahålls av unionens institutioner, byråer och organ,	(d) via en särskild portal samla, organisera och för allmänheten tillgängliggöra information om ***it-säkerhet*** som tillhandahålls av unionens institutioner, byråer och organ ***och görs tillgänglig av medlemsstaterna samt***

	offentliga och privata intressenter,

Ändringsförslag 46

Förslag till förordning
Artikel 9 – led e

Kommissionens förslag	*Ändringsförslag*
(e) öka allmänhetens medvetenhet om ***cybersäkerhetsrisker*** och ge vägledning, som är inriktad på privatpersoner och organisationer, om god praxis för enskilda användare,	(e) öka allmänhetens medvetenhet om ***it-säkerhetsrisker, sprida lämpliga åtgärder för att förhindra incidenter*** och ge vägledning, som är inriktad på privatpersoner och organisationer, om god praxis för enskilda användare,

Ändringsförslag 47

Förslag till förordning
Artikel 9 – led ea (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ea) upprätta ett nätverk av nationella utbildningskontaktpunkter som ska stödja bättre samordning och utbyte av bästa praxis bland medlemsstaterna rörande utbildning och medvetenhet om it-säkerhet,

Ändringsförslag 48

Förslag till förordning
Artikel 9 – led g

Kommissionens förslag	*Ändringsförslag*
(g) i samarbete med medlemsstaterna och unionens institutioner, organ, kontor och byråer organisera regelbundna informationskampanjer för att öka ***cybersäkerheten*** och dess synlighet i unionen.	(g) i samarbete med medlemsstaterna och unionens institutioner, organ, kontor***,*** byråer och ***andra relevanta aktörer*** organisera regelbundna informationskampanjer för att öka ***it-säkerheten*** och dess synlighet i unionen.

Ändringsförslag 49

Förslag till förordning
Artikel 9 – led ga (nytt)

Kommissionens förslag	*Ändringsförslag*
	(ga) bidra till att alla aktörer på EU:s digitala inre marknad på bred front antar förebyggande och kraftfulla it-säkerhetsåtgärder och tillförlitlig teknik för att öka skyddet av privatlivet som den första försvarslinjen mot angrepp mot informationssystem.

Motivering

Baserat på yttrandet från Europeiska datatillsynsmannen (om integritetsfrämjande teknik). Enisas roll bör tydligt sträcka sig utöver stöd till medlemsstaterna, kommissionen och EU:s byråer och bli synligare i näringslivet och för allmänheten.

Ändringsförslag 50

Förslag till förordning
Artikel 10 – led a

Kommissionens förslag	*Ändringsförslag*
(a) ge råd till unionen och medlemsstaterna om forskningsbehov och forskningsprioriteringar inom ***området cybersäkerhet***, för att möjliggöra ett effektivt svar på befintliga och nya risker och hot, bland annat när det gäller ny och framväxande informations- och kommunikationsteknik, och för att säkerställa en effektiv användning av riskförebyggande teknik,	(a) ge råd till unionen och medlemsstaterna om forskningsbehov och forskningsprioriteringar inom ***områdena it-säkerhet och skydd av personuppgifter och privatliv***, för att möjliggöra ett effektivt svar på befintliga och nya risker och hot, bland annat när det gäller ny och framväxande informations- och kommunikationsteknik, och för att säkerställa en effektiv användning av riskförebyggande teknik,

Ändringsförslag 51

Förslag till förordning
Artikel 14 – punkt 1 – led m

Kommissionens förslag	*Ändringsförslag*
(m) Utse den verkställande direktören och i förekommande fall förlänga mandatperioden för eller avsätta honom eller henne i enlighet med artikel 33 i denna förordning.	(m) ***Genom ett urvalsförfarande utgående från yrkesmässiga kriterier*** utse den verkställande direktören och i förekommande fall förlänga mandatperioden för eller avsätta honom eller henne i enlighet med artikel 33 i denna förordning.

Ändringsförslag 52

Förslag till förordning
Artikel 20 – punkt 1

Kommissionens förslag	*Ändringsförslag*
1. Styrelsen ska på förslag av den verkställande direktören inrätta en ständig intressentgrupp bestående av erkända experter som företräder berörda intressenter, exempelvis IKT-branschen, leverantörer av allmänt tillgängliga elektroniska kommunikationsnät eller kommunikationstjänster, konsumentgrupper, experter på ***cybersäkerhet*** från den akademiska världen och företrädare för behöriga myndigheter som anmälts i enlighet med [direktivet om inrättandet av en europeisk kodex för elektronisk kommunikation] samt rättsvårdande myndigheter och tillsynsmyndigheter med ansvar för dataskydd.	1. Styrelsen ska på förslag av den verkställande direktören inrätta en ständig intressentgrupp bestående av erkända experter som företräder berörda intressenter, exempelvis IKT-branschen, leverantörer av allmänt tillgängliga elektroniska kommunikationsnät eller kommunikationstjänster, konsumentgrupper, ***de europeiska standardiseringsorganisationerna,*** experter på ***it-säkerhet*** från den akademiska världen och företrädare för behöriga myndigheter som anmälts i enlighet med [direktivet om inrättandet av en europeisk kodex för elektronisk kommunikation] samt rättsvårdande myndigheter och tillsynsmyndigheter med ansvar för dataskydd.

Ändringsförslag 53

Förslag till förordning
Artikel 30 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Revisionsrätten ska ha befogenhet att utföra revision, på grundval av handlingar och kontroller på plats, hos alla stödmottagare, uppdragstagare och	*(Berör inte den svenska versionen.)*

underleverantörer som erhållit unionsfinansiering från byrån.

Ändringsförslag 54

Förslag till förordning
Artikel 44 – punkt 2

Kommissionens förslag	*Ändringsförslag*
2. Vid utarbetandet av förslag till system som avses i punkt 1 i denna artikel ska Enisa samråda med alla berörda intressenter och bedriva ett nära samarbete med gruppen. Gruppen ska ge Enisa det bistånd och de expertråd som Enisa behöver vid utarbetandet av förslaget till system, bland annat genom att avge yttranden om det behövs.	2. Vid utarbetandet av förslag till system som avses i punkt 1 i denna artikel ska Enisa samråda med alla berörda intressenter och bedriva ett nära samarbete med gruppen ***och den ständiga intressentgruppen***. Gruppen ***och den ständiga intressentgruppen*** ska ge Enisa det bistånd och de expertråd som Enisa behöver vid utarbetandet av förslaget till system, bland annat genom att avge yttranden om det behövs. ***Där så är relevant får Enisa dessutom inrätta en arbetsgrupp för intressenter avseende certifiering som består av medlemmar i den ständiga intressentgruppen och eventuella andra relevanta aktörer, som ska tillhandahålla expertrådgivning om områden som omfattas av ett särskilt förslag till system.***

Motivering

Branschen bör delta i upprättandet och utarbetandet av förslag till system, genom en samrådsprocess, i syfte att tillhandahålla sakkunskap för att säkerställa att de utformas på ett effektivt sätt.

Ändringsförslag 55

Förslag till förordning
Artikel 44 – punkt 4

Kommissionens förslag	*Ändringsförslag*
4. Med utgångspunkt i det förslag till	4. Med utgångspunkt i det förslag till

system som Enisa lagt fram, får kommissionen anta genomförandeakter i enlighet med artikel 55.1 för europeiska system för ***certifiering*** av IKT-produkter och IKT-tjänster som uppfyller kraven i artiklarna 45, 46 och 47 i denna förordning.	system som Enisa lagt fram, får kommissionen anta genomförandeakter i enlighet med artikel 55.1 för europeiska system för ***it-certifiering*** av IKT-produkter och IKT-tjänster som uppfyller kraven i artiklarna 45, 46 och 47 i denna förordning. ***Kommissionen får samråda med Europeiska dataskyddsstyrelsen och beakta dess ståndpunkt innan den antar sådana genomförandeakter.***

Motivering

Baserat på yttrandet från Europeiska datatillsynsmannen. Ändringsförslaget säkerställer överensstämmelse mellan certifieringar enligt EU-ramen för cybersäkerhetscertifiering och den allmänna dataskyddsförordningen.

Ändringsförslag 56

Förslag till förordning
Artikel 46 – punkt 2 – inledningen

Kommissionens förslag	*Ändringsförslag*
2. Assuransnivåerna grundläggande, betydande och hög ska ***uppfylla följande kriterier:***	2. Assuransnivåerna grundläggande, betydande och hög ska ***avse ett certifikat som utfärdats inom ramen för ett europeiskt system för it-säkerhetscertifiering, som ger en motsvarande grad av tillförlitlighet i fråga om påstådda eller styrkta it-säkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till dessa standarder, inbegripet tekniska kontroller, som ska minska risken för it-säkerhetsincidenter.***

Ändringsförslag 57

Förslag till förordning
Artikel 46 – punkt 2 – led a

Kommissionens förslag	*Ändringsförslag*

(a) Assuransnivån grundläggande ska avse ett certifikat som utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering, som ger en begränsad grad av tillförlitlighet i fråga om påstådda eller styrkta cybersäkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska minska risken för cybersäkerhetsincidenter.	***utgår***

Ändringsförslag 58

Förslag till förordning
Artikel 46 – punkt 2 – led b

Kommissionens förslag	*Ändringsförslag*
(b) Assuransnivån betydande ska avse ett certifikat som utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering, som ger en betydande grad av tillförlitlighet i fråga om påstådda eller styrkta cybersäkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska minska risken för cybersäkerhetsincidenter.	***utgår***

Ändringsförslag 59

Förslag till förordning
Artikel 46 – punkt 2 – led c

Kommissionens förslag	*Ändringsförslag*
(c) Assuransnivån hög ska avse ett certifikat som utfärdats inom ramen för ett europeiskt system för	***utgår***

cybersäkerhetscertifiering, som ger en högre grad av tillförlitlighet i fråga om påstådda eller styrkta cybersäkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst än certifikat med assuransnivån betydande, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska förhindra cybersäkerhetsincidenter.

Ändringsförslag 60

Förslag till förordning
Artikel 47 – punkt 1 – led aa (nytt)

Kommissionens förslag	*Ändringsförslag*
	(aa) Bedömningen av överensstämmelse och revisionsorgan.

Ändringsförslag 61

Förslag till förordning
Artikel 47 – punkt 1 – led l

Kommissionens förslag	*Ändringsförslag*
(l) Identifiering av nationella system för ***cybersäkerhetscertifiering*** som omfattar samma typ eller kategorier av IKT-produkter och IKT-tjänster.	(l) Identifiering av nationella system för ***it-säkerhetscertifiering, i enlighet med artikel 49,*** som omfattar samma typ eller kategorier av IKT-produkter och IKT-tjänster.

Ändringsförslag 62

Förslag till förordning
Artikel 48 – punkt 6

Kommissionens förslag	*Ändringsförslag*
6. Certifikat ska utfärdas för en ***period på högst tre år*** och får förnyas ***på samma villkor*** under förutsättning att de relevanta kraven fortsätter att uppfyllas.	6. Certifikat ska utfärdas för en ***maximiperiod som fastställs från fall till fall för varje system, men som inte får överstiga fem år,*** och får förnyas under

förutsättning att de relevanta kraven fortsätter att uppfyllas.

Ändringsförslag 63

Förslag till förordning
Artikel 48a (ny)

Kommissionens förslag	*Ändringsförslag*
	Artikel 48a
	Grundläggande it-säkerhetskrav
	1. Byrån ska, utgående från erfarenheterna från den ram för it-säkerhetscertifiering som avses i avdelning III i denna förordning, för kommissionen föreslå tydliga minimikrav för it-säkerhet för it-enheter som säljs i eller exporteras från unionen, såsom
	(a) att tillverkaren tillhandahåller ett skriftligt certifikat om att enheten inte innehåller någon hårdvara, programvara eller fast programvara med någon form av kända sårbarheter som kan utnyttjas i fråga om säkerhet,
	(b) att enheten bygger på programvara eller fast programvara som har kapacitet att godta på vederbörligt sätt autentiserade och tillförlitliga uppdateringar från tillverkaren,
	(c) att enheten inte innehåller något okrypterat lösenord eller okrypterad åtkomstkod, att tillverkaren dokumenterar produktens fjärråtkomstkapacitet och säkerställer den mot obehörigt tillträde, senast vid installationen, att tillverkaren inte hårdkodar standardlösenord i produkten, att säljaren dokumenterar användarnas möjligheter till uppdatering av enheterna och tydligt visar var ansvaret ligger om användaren inte uppdaterar den,
	(d) en förpliktelse för tillverkare, distributörer och importörer av internetanslutna enheter, programvaror

eller fasta programvarukomponenter att underrätta behöriga myndigheter om alla kända brister i säkerheten,

(e) en förpliktelse för tillverkare av internetanslutna enheter, programvaror eller fasta programvarukomponenter att tillhandahålla en reparation eller ersättningsenhet för varje ny säkerhetsbrist som upptäcks,

(f) en skyldighet för tillverkare av internetanslutna enheter, programvaror eller fasta programvarukomponenter att tillhandahålla information om hur enheten tar emot it-säkerhetsuppdateringar, om den förväntade tidsplanen för när it-säkerhetssupporten upphör och om vilket metod som används för att informera användaren om detta,

2. Byrån får föreslå att de minimikrav för it-säkerhet som avses i punkt 1 ska gälla för it-enheter från en eller flera specifika sektorer.

3. Byrån ska granska och, vid behov, ändra de krav för it-säkerhet som avses i punkt 1 vartannat år, samt lägga fram ändringsförslag som förslag till kommissionen.

4. Kommissionen får genom genomförandeakter och på grundval av en konsekvensbedömning besluta att de föreslagna eller ändrade it-säkerhetskrav som avses i punkterna 1 och 2 har allmän giltighet inom unionen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 55.2.

5. Kommissionen ska se till att de it-säkerhetskrav om vilka det beslutats att de har allmän giltighet enligt punkt 3 offentliggörs på lämpligt sätt.

6. Byrån ska samla in alla föreslagna it-säkerhetskrav och ändringar till dem i ett register och offentliggöra dem på lämpligt sätt.

Motivering

För att ersätta ändringsförslag 19 led c i utkastet till yttrande för tydlighetens skull. Det är viktigt att åstadkomma en motståndskraftig it-miljö för att skydda mot cyberbrottslighet och skydda it-användarnas grundläggande rättigheter. Höga it-säkerhetsmål för en obligatorisk grundläggande it-säkerhet inom unionen bör därför fastställas i denna förordning.

Ändringsförslag 64

Förslag till förordning
Artikel 50 – punkt 6 – led d

Kommissionens förslag	*Ändringsförslag*
(d) samarbeta med andra nationella tillsynsmyndigheter för certifiering eller andra myndigheter, bland annat genom att utbyta information om IKT-produkter och IKT-tjänster som eventuellt avviker från kraven i denna förordning eller särskilda europeiska system för ***cybersäkerhetscertifiering***,	(d) samarbeta med andra nationella tillsynsmyndigheter för certifiering eller andra myndigheter, ***till exempel nationella tillsynsmyndigheter för dataskydd,*** bland annat genom att utbyta information om IKT-produkter och IKT-tjänster som eventuellt avviker från kraven i denna förordning eller särskilda europeiska system för ***it-säkerhetscertifiering***,

Motivering

Från yttrandet från EDPS.

ÄRENDETS GÅNG I DET RÅDGIVANDE UTSKOTTET

Titel	Enisa, ”EU:s cybersäkerhetsbyrå”, och upphävande av förordning (EU) nr 526/2013, och cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)
Referensnummer	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Ansvarigt utskott Tillkännagivande i kammaren	ITRE 23.10.2017
Yttrande från Tillkännagivande i kammaren	LIBE 23.10.2017
Föredragande av yttrande Utnämning	Jan Philipp Albrecht 20.11.2017
Behandling i utskott	25.1.2018 8.3.2018
Antagande	8.3.2018
Slutomröstning: resultat	+: 35 –: 2 0: 4
Slutomröstning: närvarande ledamöter	Asim Ademov, Jan Philipp Albrecht, Heinz K. Becker, Caterina Chinnici, Rachida Dati, Cornelia Ernst, Kinga Gál, Sylvie Guillaume, Monika Hohlmeier, Filiz Hyusmenova, Dietmar Köster, Barbara Kudrycka, Monica Macovei, Péter Niedermüller, Ivari Padar, Judith Sargentini, Birgit Sippel, Branislav Škripek, Sergei Stanishev, Traian Ungureanu, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Auke Zijlstra
Slutomröstning: närvarande suppleanter	Maria Grapini, Sylvia-Yvonne Kaufmann, Jeroen Lenaers, Andrejs Mamikins, Maite Pagazaurtundúa Ruiz, John Procter, Jaromír Štětina, Josep-Maria Terricabras, Axel Voss, Elissavet Vozemberg-Vrionidi
Slutomröstning: närvarande suppleanter (art. 200.2)	Andrea Bocskor, Reimer Böge, André Elissen, Ramón Jáuregui Atondo, Julia Reda, Rainer Wieland, Patricija Šulin

SLUTOMRÖSTNING MED NAMNUPPROP I DET RÅDGIVANDE UTSKOTTET

35	+
ALDE	Filiz Hyusmenova, Maite Pagazaurtundúa Ruiz, Cecilia Wikström
ECR	Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Cornelia Ernst
PPE	Asim Ademov, Heinz K. Becker, Andrea Bocskor, Rachida Dati, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Jaromír Štětina, Patricija Šulin, Traian Ungureanu, Elissavet Vozemberg-Vrionidi, Rainer Wieland
S&D	Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Ramón Jáuregui Atondo, Sylvia-Yvonne Kaufmann, Dietmar Köster, Andrejs Mamikins, Péter Niedermüller, Ivari Padar, Birgit Sippel, Sergei Stanishev, Josef Weidenholzer
VERTS/ALE	Jan Philipp Albrecht, Julia Reda, Judith Sargentini, Josep-Maria Terricabras

2	-
ENF	André Elissen, Auke Zijlstra

4	0
EFDD	Kristina Winberg
PPE	Reimer Böge, Monika Hohlmeier, Axel Voss

Teckenförklaring:
+ : Ja-röster
- : Nej-röster
0 : Nedlagda röster