Europa-Parlamentet
2014-2019

Udvalget om det Indre Marked og Forbrugerbeskyttelse

2017/0225(COD)

22.5.2018

UDTALELSE

fra Udvalget om det Indre Marked og Forbrugerbeskyttelse

til Udvalget om Industri, Forskning og Energi

om forslag til Europa-Parlamentets og Rådets forordning om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed") (COM(2017)0477 – C8-0310-2017 – 2017/0225(COD))

Ordfører for udtalelse: (*) Nicola Danti

(*) Procedure med associerede udvalg – forretningsordenens artikel 54

PA_Legam

DA

KORT BEGRUNDELSE

I den digitale tidsalder er cybersikkerhed et væsentligt element for den økonomiske konkurrenceevne og sikkerhed i Den Europæiske Union og for vores frie og demokratiske samfund og de processer, der ligger til grund for dem. At sikre en høj grad af cyberrobusthed i hele EU er af afgørende betydning for at opnå forbrugernes tillid til det digitale indre marked og til yderligere udvikling af et mere innovativt og konkurrencedygtigt Europa.

Der er ingen tvivl om, at cybertrusler og globale cyberangreb - såsom "WannaCry" og "Meltdown" - er spørgsmål af stigende betydning i vores mere og mere digitaliserede samfund. Ifølge en Eurobarometerundersøgelse, som blev offentliggjort i juli 2017, betragter 87 % af respondenterne cyberkriminalitet som "en vigtig udfordring for EU's indre sikkerhed", og et flertal er "bekymret for at blive offer for forskellige former for cyberkriminalitet". Desuden har der siden begyndelsen af 2016 på verdensplan hver dag været mere end 4 000 ransom ware-angreb - en stigning på 300 % siden 2015, og 80 % af EU's virksomheder er berørt heraf. Disse kendsgerninger og resultater viser klart, at det er nødvendigt, at EU bliver mere modstandsdygtig og i stand til mere effektivt at kunne bekæmpe cyberangreb, og at EU øger sin kapacitet til at beskytte Europas borgere, virksomheder og offentlige institutioner.

Et år efter ikrafttrædelsen af direktivet om net- og informationssikkerhed forelagde Europa-Kommissionen som led i EU's strategi for cybersikkerhed en forordning, som tager sigte på yderligere at øge EU's modstandsdygtighed over for cyberangreb, afskrækkelse og forsvar. Den 13. september 2017 forelagde Kommissionen retsakten om cybersikkerhed, der hviler på to søjler:

1) et permanent og stærkere mandat for Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA), der skal bistå medlemsstaterne med effektivt at forebygge og reagere på cyberangreb, og
2) oprettelse af en ramme for EU-cybersikkerhedcertificering, der skal sikre, at IKT-produkter og -tjenester er cybersikre.

Generelt glæder ordføreren sig over den fremgangsmåde, som Kommissionen foreslår, og han støtter navnlig indførelsen af EU-dækkende certificeringsordninger for cybersikkerhed, som sigter mod at øge sikkerheden for IKT-produkter og -tjenester og undgå den bekostelige opsplitning af det indre marked på dette vigtige område. Selv om den i begyndelsen blot skulle være et frivilligt redskab, håber ordføreren, at en EU-ramme for cybersikkerhedcertificering og dertil knyttede procedurer vil blive et vigtigt redskab, der kan styrke vore borgeres og brugernes tillid og øge sikkerheden for produkter og tjenesteydelser, der cirkulerer i det indre marked.

Han er endvidere overbevist om, at en række punkter i forslaget bør præciseres og forbedres:

- Først og fremmest bør **de relevante interessenter i højere grad inddrages i de forskellige faser af styringssystemet for ENISA's udarbejdelse af forslag til certificeringsordninger**: Efter ordførerens opfattelse er det vigtigt formelt at inddrage de mest relevante interessenter såsom IKT-virksomheder, forbrugerorganisationer, SMV'er, EU's standardiseringsorganer og EU's sektorspecifikke agenturer mv. og give

dem mulighed for at komme med forslag til ordninger, rådgive ENISA med deres ekspertise og samarbejde med ENISA i forbindelse med udarbejdelsen af et forslag til ordning.

- For det andet er der behov for at udbygge den koordinerende rolle, som den europæiske cybersikkerhedscertificeringsgruppe (der består af nationale myndigheder med støtte fra Kommissionen og ENISA) varetager, og give gruppen den yderligere opgave at yde strategisk vejledning og **udarbejde et arbejdsprogram for fælles aktioner, der bør træffes på EU-plan** inden for certificering, samt at oprette og **regelmæssigt ajourføre en prioriteret liste over IKT-produkter og -tjenester,** som den mener bør omfattes af en europæisk certificeringsordning.

- Ordføreren er overbevist om, at vi bør undgå EU-certificerings"shopping", sådan som det allerede er sket i andre sektorer. **Overvågnings- og tilsynsbestemmelserne for ENISA og de nationale certificeringstilsynsmyndigheder bør skærpes væsentligt** for at sikre, at der for europæiske attester, der udstedes i én medlemsstat, gælder de samme standarder og betingelser som for dem, der er udstedt i en anden medlemsstat. Han foreslår derfor:

  1. at styrke ENISA's overvågningsbeføjelser: Sammen med certificeringsgruppen bør ENISA foretage vurderinger af de procedurer, der indføres af myndigheder med ansvar for udstedelse af EU-attester.

  2. at de nationale tilsynsmyndigheder skal foretage regelmæssige vurderinger (mindst hvert andet år) af de EU-attester, der udstedes af overensstemmelsesvurderingsorganer;

  3. at indføre fælles bindende kriterier, som skal fastlægges af gruppen, for omfanget, rækkevidden og hyppigheden af de nationale tilsynsmyndigheders vurderinger som anført i 2.

- Ordføreren mener, at der bør indføres et obligatorisk EU-tillidsmærke for certificerede IKT-produkter og -tjenester, som skal være rettet mod slutbrugerne. Et sådant mærke kan hjælpe med at øge kendskabet til cybersikkerhed og give virksomheder med god cybersikkerhed konkurrencemæssige fordele.

- Ordføreren slutter op om den ensartede og harmoniserede tilgang, som Kommissionen har anlagt, men han er overbevist om, at den bør være mere fleksibel og lettere at tilpasse til de enkelte varers og tjenesteydelsers særlige kendetegn og sårbarhed. Han afviser "one size fits all"-princippet. Derfor mener ordføreren, at betegnelserne for **sikkerhedsniveauerne** bør ændres, og at de bør tage hensyn til den påtænkte anvendelse af IKT-produkter og -tjenester. Ligeledes bør varigheden af **attesters gyldighed** fastlægges i de enkelte ordninger.

- Hver enkelt certificeringsordning bør udformes på en måde, der opmuntrer og tilskynder alle aktører, der er involveret i den pågældende sektor, til at udarbejde og fastlægge sikkerhedsstandarder, tekniske standarder og **principper om indbygget sikkerhed og privatlivsbeskyttelse** for alle faser af produkters eller tjenesteydelsers livscyklus.

ÆNDRINGSFORSLAG

Udvalget om det Indre Marked og Forbrugerbeskyttelse opfordrer Udvalget om Industri, Forskning og Energi, som er korresponderende udvalg, til at tage hensyn til følgende ændringsforslag:

Ændringsforslag 1

Forslag til forordning
Betragtning 1

Kommissionens forslag	*Ændringsforslag*
(1) Net- og informationssystemer og telekommunikationsnet og -tjenester spiller en afgørende rolle i samfundet og har udviklet sig til rygraden i den økonomiske vækst. Informations- og kommunikationsteknologier er grundlaget for de komplekse systemer, som understøtter samfundets ***aktiviteter***, og sørger for, at vore økonomier fungerer inden for vigtige sektorer såsom sundhed, energi, finans og transport, og understøtter navnlig det indre markeds funktion.	(1) Net- og informationssystemer og telekommunikationsnet og -tjenester spiller en afgørende rolle i samfundet og har udviklet sig til rygraden i den økonomiske vækst. Informations- og kommunikationsteknologier ***(IKT)*** er grundlaget for de komplekse systemer, som understøtter samfundets ***hverdagsaktiviteter***, og sørger for, at vore økonomier fungerer inden for vigtige sektorer såsom sundhed, energi, finans og transport, og understøtter navnlig det indre markeds funktion.

Ændringsforslag 2

Forslag til forordning
Betragtning 2

Kommissionens forslag	*Ændringsforslag*
(2) Borgerne, erhvervslivet og myndighederne i EU benytter i stort omfang net- og informationssystemer. Digitalisering og forbindelsesmuligheder er centrale elementer i et stadigt stigende antal produkter og tjenester og med fremkomsten af tingenes Internet (IoT) forventes millioner eller endog milliarder styk forbundet digitalt udstyr at blive udbredt i hele EU i løbet af det næste årti. Stadigt mere udstyr er forbundet til Internettet, men der tages ikke tilstrækkeligt hensyn til sikkerhed og modstandsdygtighed i udformningen,	(2) Borgerne, erhvervslivet og myndighederne i EU benytter i stort omfang net- og informationssystemer. Digitalisering og forbindelsesmuligheder er centrale elementer i et stadigt stigende antal produkter og tjenester og med fremkomsten af tingenes Internet (IoT) forventes millioner eller endog milliarder styk forbundet digitalt udstyr at blive udbredt i hele EU i løbet af det næste årti. Stadigt mere udstyr er forbundet til Internettet, men der tages ikke tilstrækkeligt hensyn til sikkerhed og modstandsdygtighed i udformningen,

hvilket medfører utilstrækkelig cybersikkerhed. I denne forbindelse fører den begrænsede anvendelse af certificering til, at organisationer og individuelle brugere får utilstrækkelige oplysninger om IKT-produkters og -tjenesters cybersikkerhedsfunktioner, hvilket undergraver tilliden til digitale løsninger.	hvilket medfører utilstrækkelig cybersikkerhed. I denne forbindelse fører den begrænsede anvendelse af certificering til, at organisationer og individuelle brugere får utilstrækkelige oplysninger om IKT-produkters og -tjenesters cybersikkerhedsfunktioner, hvilket undergraver tilliden til digitale løsninger***, der er afgørende for etableringen af det indre digitale marked***.

Ændringsforslag 3

Forslag til forordning
Betragtning 3

Kommissionens forslag	*Ændringsforslag*
(3) Øget digitalisering og konnektivitet medfører øgede cybersikkerhedsrisici, hvilket gør samfundet som helhed mere sårbart over for cybertrusler og forværrer farerne for den enkelte, herunder også sårbare individer såsom børn. For at afbøde ***denne risiko*** for samfundet bør der træffes alle nødvendige foranstaltninger for at forbedre ***cybersikkerheden*** i EU, således at net- og informationssystemer, telekommunikationsnet, digitale produkter, tjenester og udstyr, der anvendes af borgerne, myndighederne og erhvervslivet – fra SMV'er til operatører af kritisk infrastruktur – er bedre beskyttet mod cybertrusler.	(3) Øget digitalisering og konnektivitet medfører ***betydeligt*** øgede cybersikkerhedsrisici, hvilket gør samfundet som helhed mere sårbart over for cybertrusler og forværrer farerne for den enkelte, herunder også sårbare individer såsom børn. ***Forandringspotentialet i kunstig intelligens og maskinlæring vil blive udnyttet af samfundet som helhed, men også af cyberkriminelle.*** For at afbøde ***disse risici*** for samfundet bør der træffes alle nødvendige foranstaltninger for at forbedre ***sikkerheden over for cyberangreb*** i EU, således at net- og informationssystemer, telekommunikationsnet, digitale produkter, tjenester og udstyr, der anvendes af borgerne, myndighederne og erhvervslivet – fra SMV'er til operatører af kritisk infrastruktur – er bedre beskyttet mod cybertrusler.

Ændringsforslag 4

Forslag til forordning
Betragtning 4

Kommissionens forslag	*Ændringsforslag*
(4) Mængden af cyberangreb er stigende og netforbundne økonomier og samfund, som er mere sårbare over for cybertrusler og -angreb, kræver stærkere forsvarsværker. Det er dog sådan, at cyberangreb ofte er grænseoverskridende, medens den politiske respons fra cybersikkerhedsmyndigheder og retshåndhævelsesbeføjelser hovedsageligt er et nationalt anliggende. Væsentlige cyberhændelser kunne afbryde leveringen af essentielle tjenester i hele EU. Dette kræver en effektiv indsats og krisestyring på EU-plan, der bygger på målrettede politikker og vidtrækkende instrumenter for europæisk solidaritet og gensidig bistand. Det er derfor vigtigt for politikerne, erhvervslivet og brugerne, at der jævnligt foretages en vurdering af cybersikkerhedssituationen og modstandsdygtigheden i Unionen på grundlag af pålidelige EU-data samt systematiske prognoser for fremtidige udviklinger, udfordringer og trusler, både på EU-plan og globalt plan.	(4) Mængden af cyberangreb er stigende og netforbundne økonomier og samfund, som er mere sårbare over for cybertrusler og -angreb, kræver stærkere ***og sikrere*** forsvarsværker. Det er dog sådan, at cyberangreb ofte er grænseoverskridende, medens den politiske respons fra cybersikkerhedsmyndigheder og retshåndhævelsesbeføjelser hovedsageligt er et nationalt anliggende. Væsentlige cyberhændelser kunne afbryde leveringen af essentielle tjenester i hele EU. Dette kræver en effektiv indsats og krisestyring på EU-plan, der bygger på målrettede politikker og vidtrækkende instrumenter for europæisk solidaritet og gensidig bistand. Det er derfor vigtigt for politikerne, erhvervslivet og brugerne, at der jævnligt foretages en vurdering af cybersikkerhedssituationen og modstandsdygtigheden i Unionen på grundlag af pålidelige EU-data samt systematiske prognoser for fremtidige udviklinger, udfordringer og trusler, både på EU-plan og globalt plan.

Ændringsforslag 5

Forslag til forordning
Betragtning 5

Kommissionens forslag	*Ændringsforslag*
(5) I lyset af de tiltagende cybersikkerhedsudfordringer, som Unionen står over for, er der behov for et sammenhængende sæt foranstaltninger, som tager udgangspunkt i tidligere EU-tiltag og fremmer gensidigt forstærkende mål. Det omfatter behovet for yderligere at øge medlemsstaternes og virksomhedernes kapaciteter og beredskab samt at forbedre samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer. På baggrund af cybertruslers grænseoverskridende karakter	(5) I lyset af de tiltagende cybersikkerhedsudfordringer, som Unionen står over for, er der behov for et sammenhængende sæt foranstaltninger, som tager udgangspunkt i tidligere EU-tiltag og fremmer gensidigt forstærkende mål. Det omfatter behovet for yderligere at øge medlemsstaternes og virksomhedernes kapaciteter og beredskab samt at forbedre samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer. På baggrund af cybertruslers grænseoverskridende karakter

er der desuden behov for at øge kapaciteten på EU-plan, som kan supplere medlemsstaternes indsats, herunder navnlig i tilfælde af væsentlige grænseoverskridende cyberhændelser og -kriser. Der er også behov for yderligere bestræbelser på at øge borgernes og virksomhedernes kendskab til cybersikkerhed. ***Herudover bør*** tilliden til det digitale indre marked forbedres yderligere ved at give gennemsigtige oplysninger om sikkerhedsniveauet af IKT-produkter og -tjenester. Det kan fremmes ved EU-certificering***, der anvender*** fælles cybersikkerhedskrav og ***-evalueringskriterier*** på tværs af nationale markeder og sektorer.	er der desuden behov for at øge kapaciteten på EU-plan, som kan supplere medlemsstaternes indsats, herunder navnlig i tilfælde af væsentlige grænseoverskridende cyberhændelser og -kriser. Der er også behov for yderligere bestræbelser på at øge borgernes og virksomhedernes kendskab til cybersikkerhed. ***Eftersom cyberhændelser undergraver*** tilliden til ***udbydere af digitale tjenester og til selve*** det digitale indre marked***, navnlig blandt forbrugere, bør tilliden herudover*** forbedres yderligere ved at give gennemsigtige oplysninger om sikkerhedsniveauet af IKT-produkter og -tjenester. Det kan fremmes ved ***standardiseret*** EU-certificering ***på grundlag af europæiske eller internationale standarder og under anvendelse af*** fælles cybersikkerhedskrav og ***evalueringskriterier*** på tværs af nationale markeder og sektorer. ***Sideløbende med EU-dækkende certificering er der en række frivillige foranstaltninger, som den private sektor selv bør træffe for at styrke tilliden til IKT-produkters og -tjenesters sikkerhed, navnlig i lyset af det voksende udbud af IoT-enheder. For eksempel bør der gøres mere effektiv brug af kryptering og andre teknologier samt teknologier, der forhindrer vellykkede cyberangreb, herunder blockchain, med henblik på at forbedre sikkerheden for slutbrugeres data og kommunikation og den generelle sikkerhed for net- og informationssystemer i EU.***

Ændringsforslag 6

Forslag til forordning
Betragtning 5 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(5a) Selv om certificering og andre former for overensstemmelsesvurderinger af IKT-processer, -produkter og -tjenester

spiller en vigtig rolle, kræver bedre cybersikkerhed en mangefacetteret tilgang, der omfatter såvel mennesker som processer og teknologier. EU bør også fortsat i høj grad fremhæve og fremme andre bestræbelser, herunder uddannelse i cybersikkerhed og udvikling af færdigheder inden for cybersikkerhed, øget opmærksomheden på ledelses- og bestyrelsesplan, fremme af frivillig udveksling af oplysninger om cybertrusler og et skifte fra en reaktiv til en proaktiv måde at forholde sig til trusler på i EU, der fokuserer på at forhindre cyberangreb i at lykkes.

Ændringsforslag 7

Forslag til forordning
Betragtning 7

Kommissionens forslag	*Ændringsforslag*
(7) Unionen har gjort en stor indsats for at sikre cybersikkerheden og øge tilliden til de digitale teknologier. I 2013 blev EU's strategi for cybersikkerhed vedtaget for at vejlede Unionens politiske reaktion på cybersikkerhedstrusler og -risici. Som led i indsatsen for at beskytte EU's borgere bedre online vedtog Unionen i 2016 den første retsakt inden for cybersikkerhed, nemlig direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet). Ved NIS-direktivet blev der indført krav om nationale kapaciteter på cybersikkerhedsområdet, de første mekanismer til bedre strategisk og operationelt samarbejde mellem medlemsstaterne blev indført, og der blev indført forpligtelser vedrørende sikkerhedsforanstaltninger og anmeldelse af hændelser i sektorer af afgørende betydning for økonomien og samfundet såsom energi, transport, vand,	(7) Unionen har gjort en stor indsats for at sikre cybersikkerheden og øge tilliden til de digitale teknologier. I 2013 blev EU's strategi for cybersikkerhed vedtaget for at vejlede Unionens politiske reaktion på cybersikkerhedstrusler og -risici. Som led i indsatsen for at beskytte EU's borgere bedre online vedtog Unionen i 2016 den første retsakt inden for cybersikkerhed, nemlig direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet). Ved NIS-direktivet***, hvis succes i høj grad vil afhænge af, at det bliver gennemført effektivt i medlemsstaterne,*** blev der indført krav om nationale kapaciteter på cybersikkerhedsområdet, de første mekanismer til bedre strategisk og operationelt samarbejde mellem medlemsstaterne blev indført, og der blev indført forpligtelser vedrørende sikkerhedsforanstaltninger og anmeldelse af hændelser i sektorer af afgørende

bankvirksomhed, finansmarkedsinfrastrukturer, sundhed og digital infrastruktur samt for udbydere af digitale tjenester (dvs. søgemaskiner, cloud computing-tjenester og onlinemarkedspladser). ENISA fik tildelt en central rolle som støtte for gennemførelsen af dette direktiv. Hertil kommer, at den effektive bekæmpelse af cyberkriminalitet er en vigtig prioritet på den europæiske dagsorden om sikkerhed og bidrager til det overordnede mål om at nå et højere niveau af cybersikkerhed.	betydning for økonomien og samfundet såsom energi, transport, vand, bankvirksomhed, finansmarkedsinfrastrukturer, sundhed og digital infrastruktur samt for udbydere af digitale tjenester (dvs. søgemaskiner, cloud computing-tjenester og onlinemarkedspladser). ENISA fik tildelt en central rolle som støtte for gennemførelsen af dette direktiv. Hertil kommer, at den effektive bekæmpelse af cyberkriminalitet er en vigtig prioritet på den europæiske dagsorden om sikkerhed og bidrager til det overordnede mål om at nå et højere niveau af cybersikkerhed.

Ændringsforslag 8

Forslag til forordning
Betragtning 11

Kommissionens forslag	*Ændringsforslag*
(11) I betragtning af de tiltagende udfordringer på cybersikkerhedsområdet, som Unionen står over for, bør de finansielle og menneskelige ressourcer, der er tildelt Agenturet, forøges i overensstemmelse med dets udvidede rolle og opgaver og dets afgørende stilling, når det gælder forsvaret af det europæiske digitale økosystem.	(11) I betragtning af de tiltagende ***trusler og*** udfordringer på cybersikkerhedsområdet, som Unionen står over for, bør de finansielle og menneskelige ressourcer, der er tildelt Agenturet, forøges i overensstemmelse med dets udvidede rolle og opgaver og dets afgørende stilling, når det gælder forsvaret af det europæiske digitale økosystem.

Ændringsforslag 9

Forslag til forordning
Betragtning 28

Kommissionens forslag	*Ændringsforslag*
(28) Agenturet bør bidrage til at bevidstgøre offentligheden om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere og organisationer. Agenturet bør også bidrage til at fremme bedste praksis og løsninger	(28) Agenturet bør bidrage til at bevidstgøre offentligheden om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere og organisationer. Agenturet bør også bidrage til at fremme bedste praksis og løsninger

på enkeltpersons- og ***organisationsniveauet*** ved at indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og ved at sammenstille rapporter med henblik på at yde vejledning til virksomheder og borgere samt forbedre det generelle niveau af beredskab og modstandsdygtighed. Agenturet bør herudover i samarbejde med medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer tilrettelægge jævnlige informations- og oplysningskampagner for slutbrugere med sigte på at fremme en mere sikker individuel adfærd på nettet og øge bevidstheden om de potentielle farer på Internettet, herunder cyberkriminalitet, såsom phishing-angreb, botnet, økonomisk svig og banksvindel, samt fremme af grundlæggende ***autentificerings-*** og ***databeskyttelsesrådgivning***. Agenturet bør spille en central rolle i bestræbelserne på at højne slutbrugernes oplysningsniveau om udstyrs sikkerhed.

vedrørende cyberhygiejne i form af simple rutineforanstaltninger, som enkeltpersoner og organisationer kan træffe for at minimere risiciene fra cyberangreb, herunder multifaktorautentificering, patching, kryptering og ***adgangsstyring. Agenturet bør gøre dette*** ved at indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og ved at sammenstille ***og offentliggøre*** rapporter ***og retningslinjer*** med henblik på at yde vejledning til virksomheder og borgere samt forbedre det generelle niveau af beredskab og modstandsdygtighed. Agenturet bør herudover i samarbejde med medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer tilrettelægge jævnlige informations- og oplysningskampagner for slutbrugere med sigte på at fremme en mere sikker individuel adfærd på nettet og øge bevidstheden om de ***foranstaltninger, der kan træffes med henblik på at beskytte mod*** potentielle farer på Internettet, herunder cyberkriminalitet, såsom phishing-angreb, ***ransomware-angreb, hijacking,*** botnet, økonomisk svig og banksvindel, samt fremme af ***rådgivning om*** grundlæggende ***multifaktorautentificering, kryptering, patching, adgangsstyringsprincipper, databeskyttelse og andre teknologier til sikkerheds- og privatlivsbeskyttelse*** og ***anonymiseringsværktøjer***. Agenturet bør spille en central rolle i bestræbelserne på at højne slutbrugernes oplysningsniveau om udstyrs sikkerhed ***og sikker anvendelse af tjenester ved at fremme indbygget sikkerhed på EU-plan, som er altafgørende for at forbedre sikkerheden af forbundne enheder, især for sårbare slutbrugere som børn, og ved at fremme indbygget privatlivsbeskyttelse. Agenturet bør opfordre alle slutbrugere til at træffe passende foranstaltninger til at forebygge og minimere virkningen af hændelser, der påvirker sikkerheden af deres net- og informationssystemer. Der bør indgås***

partnerskaber med akademiske institutioner, der forsker i de relevante områder af cybersikkerhed.

Ændringsforslag 10

Forslag til forordning
Betragtning 35

Kommissionens forslag	*Ændringsforslag*
(35) Agenturet bør tilskynde medlemsstaterne og tjenesteudbydere til at hæve deres generelle sikkerhedsstandarder, så alle internetbrugere kan tage de nødvendige skridt til at sikre deres egen personlige cybersikkerhed. ***Navnlig bør tjenesteudbydere og produktproducenter tilbagekalde eller genbruge produkter og tjenester, som ikke overholder cybersikkerhedsstandarderne.*** I samarbejde med de kompetente myndigheder kan ENISA formidle oplysninger om cybersikkerhedsniveauet for produkter og tjenester, som udbydes i det indre marked, og udstede advarsler til udbydere og producenter og pålægge dem at forbedre sikkerheden, herunder cybersikkerheden, af deres produkter og tjenester.	(35) Agenturet bør tilskynde medlemsstaterne og tjenesteudbydere til at hæve deres generelle sikkerhedsstandarder, så alle internetbrugere kan tage de nødvendige skridt til at sikre deres egen personlige cybersikkerhed. Navnlig bør tjenesteudbydere og produktproducenter tilbagekalde eller genbruge produkter og tjenester, som ikke overholder cybersikkerhedsstandarderne. I samarbejde med de kompetente myndigheder kan ENISA formidle oplysninger om cybersikkerhedsniveauet for produkter og tjenester, som udbydes i det indre marked, og udstede advarsler til udbydere og producenter og pålægge dem at forbedre sikkerheden, herunder cybersikkerheden, af deres produkter og tjenester. ***ENISA bør offentliggøre sådanne advarsler på det websted, der tilvejebringer oplysninger om certificeringsordninger. Agenturet bør udarbejde retningslinjer om minimumssikkerhedskravene for IT-udstyr, der sælges i eller eksporteres fra Unionen. I sådanne retningslinjer kan det kræves, at producenterne afgiver en skriftlig erklæring, der bekræfter, at en anordning ikke indeholder hardware-, software- eller firmwarekomponenter med nogen kendte udnyttelige sikkerhedsmæssige sårbarheder eller nogen uforanderlige eller ukrypterede passwords eller adgangskoder, der er i stand til at modtage pålidelige og behørigt bekræftede sikkerhedsopdateringer, at sælgers svar på en berørt anordning omfatter et passende hierarki af mangelsbeføjelser, og at sælger orienterer***

slutbrugerne, når den sikkerhedsmæssige assistance ophører.

Ændringsforslag 11

Forslag til forordning
Betragtning 36 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(36a) Standarder er et frivilligt, markedsdrevet redskab med tekniske krav og retningslinjer, som er resultatet af en åben, gennemsigtig og inklusiv proces. Anvendelsen af standarder gør det lettere, at varer og tjenesteydelser er i overensstemmelse med EU-lovgivningen og støtter de europæiske politikker i overensstemmelse med forordning (EU) nr. 1025/2012 om europæisk standardisering. Agenturet bør regelmæssigt høre og samarbejde med de europæiske standardiseringsorganisationer, især i forbindelse med udarbejdelsen af europæiske cybersikkerhedscertificeringsordninger.

Ændringsforslag 12

Forslag til forordning
Betragtning 44

Kommissionens forslag	*Ændringsforslag*
(44) Agenturet bør have en stående gruppe af interessenter som et rådgivende organ, der kan sikre en løbende dialog med den private sektor, forbrugerorganisationerne og andre relevante interessenter. Den stående gruppe af interessenter, der nedsættes af bestyrelsen på forslag af den administrerende direktør, bør koncentrere sig om spørgsmål, der er relevante for interessenter, og forelægge dem for Agenturet. Sammensætningen af den	(44) Agenturet bør have en stående gruppe af interessenter som et rådgivende organ, der kan sikre en løbende dialog med den private sektor, forbrugerorganisationerne***, den akademiske verden*** og andre relevante interessenter. Den stående gruppe af interessenter, der nedsættes af bestyrelsen på forslag af den administrerende direktør, bør koncentrere sig om spørgsmål, der er relevante for interessenter, og forelægge dem for Agenturet. ***For at sikre***

stående gruppe af interessenter og de opgaver, som denne gruppe har, herunder navnlig at blive hørt i forbindelse med udkastet til arbejdsprogrammet, burde sikre en ***tilstrækkelig*** repræsentation af interessenter i Agenturets arbejde.

tilstrækkelig inddragelse af interessenter inden for rammen af cybersikkerhedscertificering bør den stående gruppe af interessenter også rådgive om, hvilke IKT-produkter og -tjenester der bør omfattes af fremtidige europæiske cybersikkerhedscertificeringsordninger, og den bør stille forslag til Kommissionen om at anmode agenturet om at udarbejde forslag til ordninger for sådanne IKT-produkter og -tjenester, enten på eget initiativ eller efter indgivelse af forslag fra relevante interessenter. Sammensætningen af den stående gruppe af interessenter og de opgaver, som denne gruppe har, herunder navnlig at blive hørt i forbindelse med udkastet til arbejdsprogrammet, burde sikre en ***effektiv og lige*** repræsentation af interessenter i Agenturets arbejde.

Ændringsforslag 13

Forslag til forordning
Betragtning 46

Kommissionens forslag	*Ændringsforslag*
(46) For at Agenturet kan sikres fuld selvstændighed og uafhængighed og for at sætte det i stand til at udføre supplerende og nye opgaver, herunder uforudsete hasteopgaver, bør Agenturet råde over et tilstrækkeligt og selvstændigt budget, hvis indtægter hovedsageligt kommer fra et bidrag fra Unionen og bidrag fra tredjelande, der deltager i Agenturets arbejde. Størstedelen af Agenturets ansatte bør være direkte involveret i den operationelle gennemførelse af Agenturets mandat. Værtsmedlemsstaten og enhver anden medlemsstat bør kunne yde frivillige bidrag til Agenturets indtægter. Unionens budgetprocedure bør finde anvendelse på ethvert bidrag, som kommer fra Unionens almindelige budget. Desuden bør revisionen af Agenturets regnskaber forestås af Revisionsretten for at sikre	(46) For at Agenturet kan sikres fuld selvstændighed og uafhængighed og for at sætte det i stand til at udføre supplerende og nye opgaver, herunder uforudsete hasteopgaver, bør Agenturet råde over et tilstrækkeligt og selvstændigt budget, hvis indtægter hovedsageligt kommer fra et bidrag fra Unionen og bidrag fra tredjelande, der deltager i Agenturets arbejde. Størstedelen af Agenturets ansatte bør være direkte involveret i den operationelle gennemførelse af Agenturets mandat. Værtsmedlemsstaten og enhver anden medlemsstat bør kunne yde frivillige bidrag til Agenturets indtægter. Unionens budgetprocedure bør finde anvendelse på ethvert bidrag, som kommer fra Unionens almindelige budget. Desuden bør revisionen af Agenturets regnskaber forestås af Revisionsretten for at sikre gennemsigtighed***,*** ansvarlighed***, effektivitet***

gennemsigtighed og ansvarlighed.	og ***omkostningseffektivitet i forbindelse med udgifter***.

Ændringsforslag 14

Forslag til forordning
Betragtning 47

Kommissionens forslag	*Ændringsforslag*
(47) Overensstemmelsesvurdering er den proces, hvorved det fastslås, om nærmere bestemte krav til et produkt, en proces, en tjeneste, et system, en person eller et organ er opfyldt. I forbindelse med denne forordning bør certificering betragtes som en form for overensstemmelsesvurdering for så vidt angår cybersikkerhedsegenskaberne for et produkt, en proces, en tjeneste, et system eller en kombination af disse ("IKT-produkter og -tjenester"), der foretages af en uafhængig tredjepart***, som ikke er produktproducenten eller tjenesteudbyderen***. Certificering kan ikke i sig selv garantere, at certificerede IKT-produkter og -tjenester er cybersikre. Det er snarere en procedure og en teknisk metode til at attestere, at IKT-produkter og -tjenester er blevet prøvet og at de opfylder visse krav til cybersikkerhed, som er fastsat andetsteds, f.eks. i tekniske standarder.	(47) Overensstemmelsesvurdering er den proces, hvorved det fastslås, om nærmere bestemte krav til et produkt, en proces, en tjeneste, et system, en person eller et organ er opfyldt. I forbindelse med denne forordning bør certificering betragtes som en form for overensstemmelsesvurdering for så vidt angår cybersikkerhedsegenskaberne ***og -praksisserne*** for et produkt, en proces, en tjeneste, et system eller en kombination af disse ("IKT-produkter og -tjenester"), der foretages af en uafhængig tredjepart ***eller ved en egenerklæring om overensstemmelse***. Certificering kan ikke i sig selv garantere, at certificerede IKT-produkter og -tjenester er cybersikre***, og slutbrugere bør gøres opmærksom på dette***. Det er snarere en procedure og en teknisk metode til at attestere, at IKT-produkter og -tjenester ***samt underliggende processer og systemer*** er blevet prøvet, og at de opfylder visse krav til cybersikkerhed, som er fastsat andetsteds, f.eks. i tekniske standarder.

Ændringsforslag 15

Forslag til forordning
Betragtning 48

Kommissionens forslag	*Ændringsforslag*
(48) ***Cybersikkerhedscertificering*** spiller en ***vigtig*** rolle for at øge tilliden til og sikkerheden af IKT-produkter og -tjenester. Det digitale indre marked og	(48) ***Den europæiske cybersikkerhedscertificering*** spiller en ***afgørende*** rolle for at øge tilliden til og sikkerheden af IKT-produkter og -tjenester.

navnlig dataøkonomien og tingenes Internet kan kun trives, hvis offentligheden generelt har tillid til, at sådanne produkter og tjenester har et ***vist*** cybersikkerhedstillidsniveau. Netforbundne og selvkørende biler, elektronisk medicinsk udstyr, industrielle automatiseringskontrolsystemer eller intelligente forsyningsnet er kun nogle eksempler på sektorer, hvor certificering allerede bruges i vidt omfang eller snart vil blive brugt. De sektorer, der reguleres af NIS-direktivet, er også sektorer, hvor cybersikkerhedscertificering er afgørende.

Det digitale indre marked og navnlig dataøkonomien og tingenes Internet kan kun trives, hvis offentligheden generelt har tillid til, at sådanne produkter og tjenester har et ***højt*** cybersikkerhedstillidsniveau. Netforbundne og selvkørende biler, elektronisk medicinsk udstyr, industrielle automatiseringskontrolsystemer eller intelligente forsyningsnet er kun nogle eksempler på sektorer, hvor certificering allerede bruges i vidt omfang eller snart vil blive brugt. De sektorer, der reguleres af NIS-direktivet, er også sektorer, hvor cybersikkerhedscertificering er afgørende.

Ændringsforslag 16

Forslag til forordning
Betragtning 50

Kommissionens forslag	*Ændringsforslag*
(50) I øjeblikket anvendes cybersikkerhedscertificering af IKT-produkter og -tjenester kun i begrænset omfang. Hvis den findes, er det som regel på medlemsstatsniveau eller inden for rammerne af en brancheordning. En attest udstedt af en national cybersikkerhedsmyndighed anerkendes i princippet ikke i andre medlemsstater. Virksomhederne kan således være nødt til at certificere deres produkter og tjenester i flere medlemsstater, hvor de driver virksomhed, f.eks. hvis de vil deltage i nationale offentlige udbud. Desuden er der, selv om der laves nye ordninger, tilsyneladende ikke nogen sammenhængende og holistisk tilgang til horisontale cybersikkerhedsspørgsmål, f.eks. inden for tingenes Internet. De bestående ordninger har væsentlige mangler og forskelle med hensyn til produktdækning, ***tillidsniveau***, materielle kriterier og den faktiske udnyttelse.	(50) I øjeblikket anvendes cybersikkerhedscertificering af IKT-produkter og -tjenester kun i begrænset omfang. Hvis den findes, er det som regel på medlemsstatsniveau eller inden for rammerne af en brancheordning. En attest udstedt af en national cybersikkerhedsmyndighed anerkendes i princippet ikke i andre medlemsstater. Virksomhederne kan således være nødt til at certificere deres produkter og tjenester i flere medlemsstater, hvor de driver virksomhed, f.eks. hvis de vil deltage i nationale offentlige udbud***, hvorved deres omkostninger øges***. Desuden er der, selv om der laves nye ordninger, tilsyneladende ikke nogen sammenhængende og holistisk tilgang til horisontale cybersikkerhedsspørgsmål, f.eks. inden for tingenes Internet. De bestående ordninger har væsentlige mangler og forskelle med hensyn til produktdækning, ***risikobaserede tillidsniveauer***, materielle kriterier og den faktiske udnyttelse.

Ændringsforslag 17

Forslag til forordning
Betragtning 52

Kommissionens forslag	*Ændringsforslag*
(52) På denne baggrund er det nødvendigt at etablere en europæisk ramme for cybersikkerhedscertificering, som fastlægger de vigtigste horisontale krav til kommende europæiske cybersikkerhedscertificeringsordninger, og som giver mulighed for anerkendelse og brug af attester for IKT-produkter og -tjenester i alle medlemsstater. Den europæiske ramme har et dobbelt formål: På den ene side bør den bidrage til at øge tilliden til IKT-produkter og -tjenester, der er certificeret i henhold til sådanne ordninger. På den anden side bør den hindre udbredelsen af modstridende eller overlappende nationale cybersikkerhedscertificeringer og dermed mindske omkostningerne for virksomheder, der opererer på det digitale indre marked. Ordningerne bør være ikke-diskriminerende og baseret på internationale eller europæiske standarder, medmindre sådanne standarder er ineffektive eller uhensigtsmæssige til at opfylde ***EU's*** legitime mål i denne henseende.	(52) På denne baggrund er det nødvendigt at ***vedtage en fælles tilgang og*** etablere en europæisk ramme for cybersikkerhedscertificering, som fastlægger de vigtigste horisontale krav til kommende europæiske cybersikkerhedscertificeringsordninger, og som giver mulighed for anerkendelse og brug af attester for IKT-produkter og -tjenester i alle medlemsstater. ***I denne forbindelse er det vigtigt at bygge videre på eksisterende nationale og internationale ordninger samt aftaler om gensidig anerkendelse, navnlig SOG-IS, og muliggøre en smidig overgang fra eksisterende ordninger under disse aftaler til ordninger under den nye europæiske ramme.*** Den europæiske ramme har et dobbelt formål: På den ene side bør den bidrage til at øge tilliden til IKT-produkter og -tjenester, der er certificeret i henhold til sådanne ordninger. På den anden side bør den hindre udbredelsen af modstridende eller overlappende nationale cybersikkerhedscertificeringer og dermed mindske omkostningerne for virksomheder, der opererer på det digitale indre marked. ***Når en europæisk cybersikkerhedscertificering har erstattet en national ordning, bør attester udstedt under den europæiske ordning godtages som værende gyldige i de tilfælde, hvor en certificering i henhold til den nationale ordning har været påkrævet.*** Ordningerne bør ***bygge på indbygget sikkerhed og principperne i forordning (EU) 2016/679. De bør desuden*** være ikke-diskriminerende og baseret på internationale eller europæiske standarder, medmindre sådanne standarder er ineffektive eller uhensigtsmæssige til at opfylde ***EU's*** legitime mål i denne henseende.

Ændringsforslag 18

Forslag til forordning
Betragtning 52 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(52a) Den europæiske ramme for cybersikkerhedscertificering bør etableres på en ensartet måde i alle medlemsstater med henblik på at undgå "certificeringsshopping" som følge af forskelle mellem medlemsstaterne med hensyn til omkostninger eller krav af forskellig strenghed.

Ændringsforslag 19

Forslag til forordning
Betragtning 55

Kommissionens forslag	*Ændringsforslag*
(55) Målet med europæiske cybersikkerhedscertificeringsordninger ***er*** at sikre, at de IKT-produkter og -tjenester, der er certificeret i overensstemmelse med en ***sådan*** ordning, opfylder de fastsatte krav. Kravene vedrører evnen til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse ***produkter,*** processer, tjenester og systemer i denne forordnings betydning. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-produkter og -tjenester i denne forordning. IKT-produkter og -tjenester og de tilhørende cybersikkerhedsbehov er så forskellige, at det er meget vanskeligt at komme med generelle cybersikkerhedskrav, der gælder for alting.	(55) Målet med europæiske cybersikkerhedscertificeringsordninger ***bør være*** at ***bidrage til større beskyttelse af slutbrugerne og af den europæiske konkurrenceevne samt højne sikkerhedsniveauet på det digitale indre marked og mere konkret*** sikre, at de IKT-produkter og -tjenester, der er certificeret i overensstemmelse med en ordning, opfylder de fastsatte krav. Kravene vedrører evnen til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse processer***, produkter***, tjenester og systemer i denne forordnings betydning. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-produkter og -tjenester i denne forordning.

Det er således nødvendigt at have en bred og generel opfattelse af cybersikkerhed med henblik på certificering, som suppleres af en række specifikke cybersikkerhedsmål, som skal tages i betragtning ved udformningen af europæiske cybersikkerhedscertificeringsordninger. De metoder, der skal anvendes til at nå disse mål for specifikke IKT-produkter og -tjenester bør så præciseres yderligere i den enkelte certificeringsordning, der vedtages af Kommissionen, f.eks. i form af henvisninger til standarder eller tekniske specifikationer.	IKT-produkter og -tjenester og de tilhørende cybersikkerhedsbehov er så forskellige, at det er meget vanskeligt at komme med generelle cybersikkerhedskrav, der gælder for alting. Det er således nødvendigt at have en bred og generel opfattelse af cybersikkerhed med henblik på certificering, som suppleres af en række specifikke cybersikkerhedsmål, som skal tages i betragtning ved udformningen af europæiske cybersikkerhedscertificeringsordninger. De metoder, der skal anvendes til at nå disse mål for specifikke IKT-produkter og -tjenester bør så præciseres yderligere i den enkelte certificeringsordning, der vedtages af Kommissionen, f.eks. i form af henvisninger til standarder eller tekniske specifikationer. ***Det har afgørende betydning, at hver enkel europæiske cybersikkerhedscertificeringsordning udformes på en måde, der opmuntrer og tilskynder alle aktører, der er involveret i den pågældende sektor, til at udvikle og vedtage sikkerhedsstandarder, tekniske normer og principper om indbygget sikkerhed for alle faser af produkternes eller tjenesteydelsernes livscyklus. Hvis certificeringsordningen fastsætter mærker eller etiketter, skal betingelserne for anvendelsen af disse mærker eller etiketter beskrives. Et sådant mærke, som kan være i form af et digitalt logo eller en QR-kode, bør angive de risici, der er forbundet med driften og brugen af IKT-produkter og -tjenester, og bør være klart og letforståeligt for forbrugerne.***

Ændringsforslag 20

Forslag til forordning
Betragtning 55 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(55a) I lyset af innovationstendenserne, den voksende tilgængelighed og det

konstant stigende antal IoT-enheder i alle samfundssektorer bør opmærksomheden navnlig rettes mod sikkerheden for alle og selv de mest simple IoT-produkter. Da certificering er en vigtig metode til at øge tilliden til markedet og styrke sikkerheden og modstandskraften, bør der lægges vægt på IoT-produkter og -tjenester i den nye EU-ramme for cybersikkerhedscertificering, så de bliver mindre sårbare og mere sikre for forbrugere og virksomheder.

Ændringsforslag 21

Forslag til forordning
Betragtning 56

Kommissionens forslag	*Ændringsforslag*
(56) ***Kommissionen*** bør ***have beføjelse til at anmode ENISA om at udarbejde forslag til ordninger for specifikke IKT-produkter eller -tjenester. Kommissionen bør på grundlag af den af ENISA foreslåede ordning have beføjelse*** til ***at vedtage den europæiske cybersikkerhedscertificeringsordning ved hjælp af gennemførelsesretsakter***. Under hensyntagen til de generelle formål og sikkerhedsmål, der er fastsat i denne forordning, bør europæiske cybersikkerhedscertificeringsordninger, der vedtages af Kommissionen, angive et minimumssæt af elementer vedrørende den enkelte ordnings genstand, omfang og funktion. Det bør bl.a. omfatte cybersikkerhedscertificeringens omfang og genstand, herunder de omfattede kategorier af IKT-produkter og -tjenester, nærmere specifikation af cybersikkerhedskravene, f.eks. med henvisning til standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder og det påtænkte tillidsniveau ***(***dvs. ***grundlæggende***, betydeligt eller ***højt)***.	(56) ***ENISA*** bør ***drive et særligt websted med et letanvendeligt internetbaseret værktøj med oplysninger om vedtagne ordninger, forslag*** til ***ordninger og ordninger, som Kommissionen har anmodet om***. Under hensyntagen til de generelle formål og sikkerhedsmål, der er fastsat i denne forordning, bør europæiske cybersikkerhedscertificeringsordninger, der vedtages af Kommissionen, angive et minimumssæt af elementer vedrørende den enkelte ordnings genstand, omfang og funktion. Det bør bl.a. omfatte cybersikkerhedscertificeringens omfang og genstand, herunder de omfattede kategorier af IKT-produkter og -tjenester, nærmere specifikation af cybersikkerhedskravene, f.eks. med henvisning til standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder***, der er forbundet med driften og brugen af et IKT-produkt, en IKT-proces eller en IKT-tjeneste, deres iboende risiko*** og det påtænkte tillidsniveau***: funktionelt sikkert,*** dvs. ***tillidsniveauer med et funktionelt sikkerhedsniveau***, betydeligt ***sikkert, særdeles sikkert*** eller ***en kombination heraf. Tillidsniveauerne bør ikke skabe en***

formodning om absolut sikkerhed, således at slutbrugeren ikke vildledes. Der bør også tages hensyn til hele produktets livscyklus. Med henblik på at klarlægge, hvilke risici en bestemt vare eller tjeneste er udformet til at kunne modstå, bør ENISA koordinere udarbejdelsen af en tjekliste over de risici, som IKT-processen, -produktet eller -tjenesten forventes udsat for af en bestemt kategori af brugere i et bestemt miljø.

Ændringsforslag 22

Forslag til forordning
Betragtning 56 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(56 a) Kommissionen bør have beføjelse til at anmode ENISA om at udarbejde forslag til ordninger for specifikke IKT-produkter eller -tjenester. Beføjelsen til at vedtage retsakter i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde bør delegeres til Kommissionen med henblik på at etablere europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelsen af delegerede retsakter. I forbindelse med vedtagelsen af disse delegerede retsakter bør Kommissionen basere

cybersikkerhedscertificeringsordningerne for IKT-produkter og -tjenester på relevante kandidatordninger foreslået af ENISA med henblik på at fremme tilliden til og forudsigeligheden af cybersikkerhedscertificeringsrammen og bevidstgøre offentligheden om den.

Ændringsforslag 23

Forslag til forordning
Betragtning 56 b (ny)

Kommissionens forslag	*Ændringsforslag*
	(56b) Blandt de evalueringsmetoder og vurderingsprocedurer, som vedrører de enkelte europæiske cybersikkerhedscertificeringsordninger, bør etisk hacking, som har til formål at lokalisere svagheder og sårbarheder i enheder og informationssystemer ved at forudsige ondsindede hackeres intentioner og færdigheder, fremmes på EU-plan.

Ændringsforslag 24

Forslag til forordning
Betragtning 58

Kommissionens forslag	*Ændringsforslag*
(58) Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenterne af IKT-produkter og udbydere af IKT-tjenester indgive en ansøgning om certificering af deres produkter eller tjenester til et overensstemmelsesvurderingsorgan efter eget valg. Overensstemmelsesvurderingsorganer bør akkrediteres af et akkrediteringsorgan, hvis de opfylder visse nærmere fastsatte krav i denne forordning. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt	(58) Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenterne af IKT-produkter og udbydere af IKT-tjenester indgive en ansøgning om certificering af deres ***processer,*** produkter eller tjenester til et overensstemmelsesvurderingsorgan efter eget valg***, eller de kan afgive en egenerklæring om, at deres produkter eller tjenester er i overensstemmelse med den relevant europæiske cybersikkerhedscertificeringsordning***. Overensstemmelsesvurderingsorganer bør akkrediteres af et akkrediteringsorgan, hvis

overensstemmelsesvurderingsorganet opfylder kravene. Akkrediteringsorganer tilbagekalder akkrediteringen af et overensstemmelsesvurderingsorgan, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis foranstaltninger truffet af et overensstemmelsesvurderingsorgan er i modstrid med denne forordning.

de opfylder visse nærmere fastsatte krav i denne forordning. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt overensstemmelsesvurderingsorganet opfylder kravene. Akkrediteringsorganer tilbagekalder akkrediteringen af et overensstemmelsesvurderingsorgan, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis foranstaltninger truffet af et overensstemmelsesvurderingsorgan er i modstrid med denne forordning. ***Med henblik på at sikre, at akkreditering foretages på en ensartet måde i hele Den Europæiske Union, bør de nationale certificeringstilsynsmyndigheder være underlagt en fagfællebedømmelse vedrørende de procedurer, der kontrollerer overensstemmelsen af produkterne, der er underlagt en cybersikkerhedscertificering.***

Ændringsforslag 25

Forslag til forordning
Betragtning 59

Kommissionens forslag	*Ændringsforslag*
(59) Det er nødvendigt at pålægge alle medlemsstater at udpege en tilsynsmyndighed for cybercertificering, som skal føre tilsyn med overensstemmelsesvurderingsorganernes overholdelse af reglerne og med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, samt overholdelse af kravene i denne forordning og de relevante cybersikkerhedscertificeringsordninger. Nationale certificeringstilsynsmyndigheder bør behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, undersøge	(59) Det er nødvendigt at pålægge alle medlemsstater at udpege en tilsynsmyndighed for cybercertificering, som skal føre tilsyn med overensstemmelsesvurderingsorganernes overholdelse af reglerne og med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, samt overholdelse af kravene i denne forordning og de relevante cybersikkerhedscertificeringsordninger. Nationale certificeringstilsynsmyndigheder bør behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, undersøge

genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist. Herudover samarbejder de med andre certificeringstilsynsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings krav eller specifikke cybersikkerhedscertificeringsordninger.	genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist. Herudover samarbejder de med andre certificeringstilsynsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings krav eller specifikke cybersikkerhedscertificeringsordninger. ***Derudover bør de overvåge og kontrollere efterlevelsen af egenerklæringerne om overensstemmelse, og at der er udstedt europæiske cybersikkerhedscertifikater af overensstemmelsesvurderingsorganer med de krav, der er fastsat i denne forordning, herunder den europæiske cybersikkerhedscertificeringsgruppes regler og kravene i den tilsvarende europæiske cybersikkerhedscertificeringsordning. Et effektivt samarbejde mellem de nationale certificeringstilsynsmyndigheder er afgørende for at opnå en korrekt gennemførelse af europæiske cybersikkerhedscertificeringsordninger og tekniske spørgsmål vedrørende IKT-produkters og -tjenesters cybersikkerhed. Kommissionen bør lette denne udveksling af oplysninger ved at stille et generelt understøttende elektronisk informationssystem til rådighed, f.eks. informations- og kommunikationssystemet for markedsovervågning (ICSMS) og det hurtige varslingssystem for farlige nonfoodprodukter (RAPEX), som allerede anvendes af markedsovervågningsmyndighederne i medfør af forordning (EF) nr. 765/2008.***

Ændringsforslag 26

Forslag til forordning
Betragtning 63

Kommissionens forslag	*Ændringsforslag*
(63) Med sigte på at fastsætte de nærmere kriterier for akkrediteringen af overensstemmelsesvurderingsorganer bør Kommissionen tillægges beføjelser til at vedtage retsakter i henhold til artikel 290 i traktaten om Den Europæiske Unions Funktionsmåde. Kommissionen bør under sit forberedende arbejde gennemføre relevante høringer, herunder på ekspertniveau. Disse høringer bør gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016. For at sikre lige deltagelse i forberedelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.	***udgår***

Ændringsforslag 27

Forslag til forordning
Betragtning 65

Kommissionens forslag	*Ændringsforslag*
(65) Undersøgelsesproceduren bør anvendes til at vedtage gennemførelsesretsakter om de europæiske cybersikkerhedscertificeringsordninger for ***IKT-produkter*** og -tjenester, om Agenturets metoder i forbindelse med gennemførelsen af undersøgelser, samt om vilkår, formater og procedurer for de nationale certificeringstilsynsmyndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer til Kommissionen.	(65) Undersøgelsesproceduren bør anvendes til at vedtage gennemførelsesretsakter om de europæiske cybersikkerhedscertificeringsordninger for ***IKT-processer, -produkter*** og -tjenester, om Agenturets metoder i forbindelse med gennemførelsen af undersøgelser, samt om vilkår, formater og procedurer for de nationale certificeringstilsynsmyndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer til Kommissionen ***under hensyntagen til den dokumenterede effektivitet af det elektroniske notifikationsværktøj "New Approach Notified and Designated***

Organisations" (NANDO).

Ændringsforslag 28

Forslag til forordning
Betragtning 66

Kommissionens forslag	*Ændringsforslag*
(66) Der bør foretages en uafhængig evaluering af Agenturets arbejde. Evalueringen bør ***tage stilling til***, om Agenturets ***mål nås***, om ***arbejdsmetoderne er effektive***, og om dets opgaver er relevante. Evalueringen bør også vurdere virkningen, effektiviteten og omkostningseffektiviteten af den europæiske ramme for cybersikkerhedscertificering.	(66) Der bør foretages en uafhængig evaluering af Agenturets arbejde. Evalueringen bør ***indeholde en vurdering af***, om Agenturets ***udgifter er legitime og effektive***, ***og*** om ***det når sine mål på effektiv vis***, ***ligesom den bør omfatte en beskrivelse af dets arbejdsmetoder*** og ***en vurdering af,*** om dets opgaver er relevante. Evalueringen bør også vurdere virkningen, effektiviteten og omkostningseffektiviteten af den europæiske ramme for cybersikkerhedscertificering.

Ændringsforslag 29

Forslag til forordning
Artikel 2 – stk. 1 – nr. 1

Kommissionens forslag	*Ændringsforslag*
(11) ***"IKT-produkter*** og ***tjenester"***: ***ethvert element*** eller ***enhver gruppe af elementer*** i net- og informationssystemer	(11) ***"IKT-processer, -produkter*** og ***-tjenester"***: ***et produkt, en tjeneste, en proces, et system*** eller ***en kombination heraf, som er et element*** i net- og informationssystemer ***(Dette ændringsforslag gælder for hele teksten. Hvis det vedtages, skal ændringerne foretages alle de berørte steder).***

Ændringsforslag 30

Forslag til forordning
Artikel 2 – stk. 1 – nr. 11 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	(11 a) "national certificeringstilsynsmyndighed": en myndighed i en medlemsstat, der er ansvarlig for at udføre overvågnings-, håndhævelses- og tilsynsopgaver i forbindelse med cybersikkerhedscertificering på medlemsstatens område;

Ændringsforslag 31

Forslag til forordning
Artikel 2 – stk. 1 – nr. 16 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	(16 a) "egenerklæring om overensstemmelse": en erklæring fra producenten om, at dennes IKT-proces, -produkt eller -tjeneste er i overensstemmelse med en specifik europæisk cybersikkerhedscertificeringsordning.

Ændringsforslag 32

Forslag til forordning
Artikel 3 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Agenturet udfører de opgaver, det tillægges ved nærværende forordning, med det formål at bidrage til et højt cybersikkerhedsniveau i Unionen.	1. Agenturet udfører de opgaver, det tillægges ved nærværende forordning, med det formål at bidrage til ***at opnå*** et højt ***fælles*** cybersikkerhedsniveau***, således at cyberangreb*** i Unionen ***forebygges, fragmentering på det indre marked mindskes, og dets funktion forbedres***.

Ændringsforslag 33

Forslag til forordning
Artikel 4 – stk. 5

Kommissionens forslag	*Ændringsforslag*
5. Agenturet ***øger*** cybersikkerhedskapaciteten på EU-plan for at supplere medlemsstaternes indsats for at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser.	5. Agenturet ***bidrager til at øge*** cybersikkerhedskapaciteten på EU-plan for at supplere ***og styrke*** medlemsstaternes indsats for at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser.

Ændringsforslag 34

Forslag til forordning
Artikel 4 – stk. 6

Kommissionens forslag	*Ændringsforslag*
6. Agenturet fremmer brugen af certificering***, herunder ved at bidrage*** til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau, jf. ***afsnit III***, for at øge gennemsigtigheden af IKT-produkters og -tjenesters cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked.	6. Agenturet fremmer brugen af certificering ***og undgår samtidig fragmentering som følge af manglende koordinering mellem eksisterende certificeringsordninger i Unionen. Agenturet bidrager*** til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau, jf. ***artikel 43 til 54 [afsnit III]***, for at øge gennemsigtigheden af IKT-produkters og -tjenesters cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked.

Ændringsforslag 35

Forslag til forordning
Artikel 4 – stk. 7

Kommissionens forslag	*Ændringsforslag*
7. Agenturet fremmer et højt niveau for oplysning af borgere og virksomheder vedrørende cybersikkerhed.	7. Agenturet fremmer et højt niveau for oplysning af borgere***, myndigheder*** og virksomheder vedrørende cybersikkerhed.

Ændringsforslag 36

Forslag til forordning
Artikel 5 – stk. 1 – nr. 1

Kommissionens forslag	*Ændringsforslag*
1. bistå og rådgive***, navnlig ved at levere uafhængige udtalelser og forberedende arbejde,*** ved udvikling og revision af Unionens politik og lovgivning på cybersikkerhedsområdet samt sektorspecifik politik og lovgivningsinitiativer, som involverer cybersikkerhedsanliggender	1. bistå og rådgive ved udvikling og revision af Unionens politik og lovgivning på cybersikkerhedsområdet samt sektorspecifik politik og lovgivningsinitiativer, som involverer cybersikkerhedsanliggender

Begrundelse

Agenturet bør frit kunne vælge, hvilke instrumenter det vil bruge til at udføre sine opgaver.

Ændringsforslag 37

Forslag til forordning
Artikel 5 – stk. 1 – nr. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. bistå Det Europæiske Databeskyttelsesråd, som blev oprettet ved forordning (EU) 2016/679, med at udarbejde retningslinjer, som skal angive de tekniske betingelser for, at registeransvarlige lovligt kan anvende personoplysninger af IT-sikkerhedshensyn med det formål at beskytte deres infrastruktur ved at spore og blokere angreb mod deres informationssystemer i forbindelse med: i) forordning (EU)2016/679[1a], ii) direktiv (EU) 2016/1148[1b], og iii) direktiv 2002/58/EF[1c];
	1a Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016,

s. 1).

1b Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

1c Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

Begrundelse

Etablering af egentlige samarbejdsmekanismer.

Ændringsforslag 38

Forslag til forordning
Artikel 5 – stk. 1 – nr. 4 – nr. 2

Kommissionens forslag	*Ændringsforslag*
(2) fremme af et højere sikkerhedsniveau i elektronisk kommunikation, herunder gennem rådgivning og bistand samt ved at fremme udvekslingen af bedste praksis mellem de kompetente myndigheder	(2) fremme af et højere sikkerhedsniveau i elektronisk kommunikation, ***dataopbevaring og databehandling,*** herunder gennem rådgivning og bistand samt ved at fremme udvekslingen af bedste praksis mellem de kompetente myndigheder

Ændringsforslag 39

Forslag til forordning
Artikel 6 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. Agenturet letter oprettelsen og lanceringen af et langsigtet europæisk

	cybersikkerhedsprojekt med henblik på at støtte fremvæksten af en uafhængig EU-cybersikkerhedsindustri og integrere cybersikkerhed i hele EU's udvikling på IKT-området.

Begrundelse

ENISA bør rådgive lovgiverne om udarbejdelsen af politikker, således at EU kan komme op på niveau med IT-sikkerhedsindustrierne i tredjelande. Projektets omfang skal være sammenligneligt med det, der tidligere er opnået i luftfartsindustrien (f.eks. Airbus). Dette er nødvendigt for at udvikle en stærkere, suveræn og troværdig IKT-industri i EU (se undersøgelsen fra Enheden for Videnskabeligt Fremsyn (STOA) PE 614.531).

Ændringsforslag 40

Forslag til forordning
Artikel 7 – stk. 5 – afsnit 1

Kommissionens forslag	*Ændringsforslag*
På anmodning af ***to*** eller flere berørte medlemsstater og alene med det formål at levere rådgivning om forebyggelse af fremtidige hændelser skal Agenturet yde støtte til eller foretage en efterfølgende teknisk undersøgelse efter underretning fra de berørte virksomheder om hændelser, der har en betydelig eller væsentlig virkning, i henhold til direktiv (EU) 2016/1148. Agenturet skal også foretage en sådan undersøgelse efter en behørigt begrundet anmodning fra Kommissionen og efter aftale med de berørte medlemsstater i tilfælde, hvor flere end to medlemsstater berøres af sådanne hændelser.	På anmodning af ***en*** eller flere berørte medlemsstater og alene med det formål at levere rådgivning om forebyggelse af fremtidige hændelser skal Agenturet yde støtte til eller foretage en efterfølgende teknisk undersøgelse efter underretning fra de berørte virksomheder om hændelser, der har en betydelig eller væsentlig virkning, i henhold til direktiv (EU) 2016/1148. Agenturet skal også foretage en sådan undersøgelse efter en behørigt begrundet anmodning fra Kommissionen og efter aftale med de berørte medlemsstater i tilfælde, hvor flere end to medlemsstater berøres af sådanne hændelser.

Ændringsforslag 41

Forslag til forordning
Artikel 7 – stk. 8 – litra a

Kommissionens forslag	*Ændringsforslag*
a) sammenstille rapporter fra nationale kilder med henblik på at bidrage til at	a) sammenstille rapporter fra nationale ***og internationale*** kilder med henblik på at

skabe en fælles situationsforståelse	bidrage til at skabe en fælles situationsforståelse

Ændringsforslag 42

Forslag til forordning
Artikel 8 – stk. 1 – litra a – nr. 1 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	(1a) i samarbejde med den europæiske cybersikkerhedscertificeringsgruppe udføre vurderinger af procedurerne for udstedelse af europæiske cybersikkerhedsattester, der er indført af de i artikel 51 omhandlede overensstemmelsesvurderingsorganer, med henblik på at sikre, at overensstemmelsesvurderingsorganerne anvender denne forordning på en ensartet måde, når de udsteder attester

Ændringsforslag 43

Forslag til forordning
Artikel 8 – stk. 1 – litra a – nr. 1 b (nyt)

Kommissionens forslag	*Ændringsforslag*
	(1b) udføre uafhængige periodiske efterfølgende kontroller af, om certificerede IKT-produkter og -tjenester overholder de europæiske cybersikkerhedscertificeringsordninger

Ændringsforslag 44

Forslag til forordning
Artikel 8 – stk. 1 – litra a – nr. 3

Kommissionens forslag	*Ændringsforslag*
(3) samle og offentliggøre retningslinjer og udvikle god praksis vedrørende cybersikkerhedskrav til IKT-	(3) samle og offentliggøre retningslinjer og udvikle god praksis***, herunder om principper for cyberhygiejne***

produkter og -tjenester i samarbejde med nationale certificeringstilsynsmyndigheder og branchen	***og om ikke at anvende hemmelige bagdøre,*** vedrørende cybersikkerhedskrav til IKT-produkter og -tjenester i samarbejde med nationale certificeringstilsynsmyndigheder og branchen ***i en formaliseret, standardiseret og gennemsigtig proces***

Ændringsforslag 45

Forslag til forordning
Artikel 8 – stk. 1 – litra b

Kommissionens forslag	*Ændringsforslag*
b) ***fremme*** indførelse og udbredelse af europæiske og internationale standarder for risikostyring og sikkerhed af IKT-produkter og -tjenester og i samarbejde med medlemsstaterne udarbejde vejledning og retningslinjer om de tekniske områder vedrørende sikkerhedskrav for operatører af væsentlige tjenester og udbydere af digitale tjenester samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, i henhold til artikel 19, stk. 2, i direktiv (EU) 2016/1148	b) ***høre de europæiske standardiseringsorganer og europæiske standardiseringsorganisationer om udviklingen af standarder for at sikre, at de standarder, der anvendes i europæiske cybersikkerhedscertificeringsordninger, er hensigtsmæssige, og fremme*** indførelse og udbredelse af ***relevante*** europæiske og internationale standarder for risikostyring og sikkerhed af IKT-produkter og -tjenester og i samarbejde med medlemsstaterne udarbejde vejledning og retningslinjer om de tekniske områder vedrørende sikkerhedskrav for operatører af væsentlige tjenester og udbydere af digitale tjenester samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, i henhold til artikel 19, stk. 2, i direktiv (EU) 2016/1148

Ændringsforslag 46

Forslag til forordning
Artikel 8 – stk. 1 – litra b a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ba) udarbejde retningslinjer for, hvordan og hvornår medlemsstaterne skal informere hinanden, når de får kendskab

	til en offentligt ukendt sårbarhed i IKT-processen, -produktet eller -tjenesten, som er certificeret i overensstemmelse med denne forordnings afsnit III, herunder retningslinjer om politikker for koordineret formidling af sårbarheder

Ændringsforslag 47

Forslag til forordning
Artikel 8 – stk. 1 – litra b b (nyt)

Kommissionens forslag	*Ændringsforslag*
	bb) udarbejde retningslinjer om minimumssikkerhedskravene for IT-udstyr, der sælges på EU's marked eller eksporteres fra EU

Ændringsforslag 48

Forslag til forordning
Artikel 9 – stk. 1 – litra d

Kommissionens forslag	*Ændringsforslag*
d) via en særlig webportal samle, organisere og offentliggøre oplysninger om cybersikkerhed, der leveres af Unions institutioner, agenturer og organer	d) via en særlig webportal samle, organisere og offentliggøre oplysninger om cybersikkerhed, der leveres af Unions institutioner, agenturer og organer**,** ***herunder oplysninger om væsentlige cybersikkerhedshændelser og større brud på datasikkerheden***

Ændringsforslag 49

Forslag til forordning
Artikel 9 – stk. 1 – litra e

Kommissionens forslag	*Ændringsforslag*
e) højne offentlighedens oplysningsniveau om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for ***individuelle brugere, der er målrettet mod borgere*** og ***organisationer***	e) højne offentlighedens oplysningsniveau om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for ***borgere og organisationer samt fremme vedtagelsen af forebyggende***

	stærke IT-sikkerhedsforanstaltninger og ***pålidelig databeskyttelse og beskyttelse af privatlivets fred;***

Ændringsforslag 50

Forslag til forordning
Artikel 9 – stk. 1 – litra g a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ga) støtte tættere samarbejde og udveksling af bedste praksis mellem medlemsstaterne vedrørende cybersikkerhedsuddannelse, cyberhygiene og bevidstgørelse;

Ændringsforslag 51

Forslag til forordning
Artikel 10 – stk. 1 – litra a

Kommissionens forslag	*Ændringsforslag*
a) ***rådgive*** Unionen og medlemsstaterne om forskningsbehov på cybersikkerhedsområdet med henblik på at gøre det muligt effektivt at imødegå nuværende og kommende risici og -trusler, herunder hvad angår nye og kommende informations- og kommunikationsteknologier, og effektivt bruge risikoforebyggende teknologier	a) ***sikre forudgående høring af relevante brugergrupper og rådgive*** Unionen og medlemsstaterne om forskningsbehov på cybersikkerhedsområdet med henblik på at gøre det muligt effektivt at imødegå nuværende og kommende risici og -trusler, herunder hvad angår nye og kommende informations- og kommunikationsteknologier, og effektivt bruge risikoforebyggende teknologier***;***

Ændringsforslag 52

Forslag til forordning
Artikel 13 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Bestyrelsen består af en repræsentant for hver medlemsstat og to repræsentanter, der udnævnes af Kommissionen. Alle repræsentanter har	1. Bestyrelsen består af en repræsentant for hver medlemsstat og to repræsentanter, der udnævnes af Kommissionen ***og Europa-Parlamentet***.

stemmeret.	Alle repræsentanter har stemmeret.

Ændringsforslag 53

Forslag til forordning
Artikel 14 – stk. 1 – litra e

Kommissionens forslag	*Ændringsforslag*
e) evaluere og vedtage den konsoliderede årsberetning om Agenturets virksomhed og sende både rapporten og bestyrelsens evaluering til Europa-Parlamentet, Rådet, Kommissionen og Revisionsretten senest den 1. juli i det følgende år. Årsberetningen skal indeholde regnskaberne og ***beskrive***, i hvilket omfang ***Agenturet*** har opfyldt sine resultatindikatorer. Årsberetningen offentliggøres	e) evaluere og vedtage den konsoliderede årsberetning om Agenturets virksomhed og sende både rapporten og bestyrelsens evaluering til Europa-Parlamentet, Rådet, Kommissionen og Revisionsretten senest den 1. juli i det følgende år. Årsberetningen skal indeholde regnskaberne***, beskrive omkostningseffektiviteten*** og ***vurdere***, ***hvor effektivt Agenturet har været, og*** i hvilket omfang ***det*** har opfyldt sine resultatindikatorer. Årsberetningen offentliggøres

Ændringsforslag 54

Forslag til forordning
Artikel 14 – stk. 1 – litra m

Kommissionens forslag	*Ændringsforslag*
m) udnævne den administrerende direktør og, hvis relevant, forlænge den administrerende direktørs ansættelsesperiode eller afskedige vedkommende i overensstemmelse med denne forordnings artikel 33	m) udnævne den administrerende direktør ***gennem udvælgelse baseret på faglige kriterier*** og, hvis relevant, forlænge den administrerende direktørs ansættelsesperiode eller afskedige vedkommende i overensstemmelse med denne forordnings artikel 33

Ændringsforslag 55

Forslag til forordning
Artikel 14 – stk. 1 – litra o

Kommissionens forslag	*Ændringsforslag*
o) træffe alle afgørelser vedrørende etablering af Agenturets organisatoriske	o) træffe alle afgørelser vedrørende etablering af Agenturets organisatoriske

struktur og om nødvendigt ændring heraf under hensyntagen til Agenturets aktivitetsbehov og under hensyntagen til forsvarlig budgetforvaltning	struktur og om nødvendigt ændring heraf under hensyntagen til Agenturets aktivitetsbehov ***som anført i denne forordning*** og under hensyntagen til forsvarlig budgetforvaltning

Ændringsforslag 56

Forslag til forordning
Artikel 19 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Den administrerende direktør aflægger rapport til Europa-Parlamentet om udførelsen af sit hverv, når denne anmodes herom. Rådet kan anmode den administrerende direktør om at aflægge rapport om udførelsen af dennes hverv.	2. Den administrerende direktør aflægger ***årligt*** rapport til Europa-Parlamentet om udførelsen af sit hverv, når denne anmodes herom. Rådet kan anmode den administrerende direktør om at aflægge rapport om udførelsen af dennes hverv.

Ændringsforslag 57

Forslag til forordning
Artikel 20 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. På forslag af den administrerende direktør nedsætter bestyrelsen en stående gruppe af interessenter bestående af anerkendte eksperter, der repræsenterer de relevante interessenter såsom IKT-industrien, udbydere af elektroniske kommunikationsnet og -tjenester til offentligheden, forbrugergrupper, akademiske eksperter i ***cybersikkerhed*** og repræsentanter for de kompetente myndigheder, der er givet meddelelse om i henhold til [direktiv om en europæisk kodeks for elektronisk kommunikation], samt retshåndhævende myndigheder og databeskyttelsestilsynsmyndigheder.	1. På forslag af den administrerende direktør nedsætter bestyrelsen en stående gruppe af interessenter bestående af anerkendte eksperter, der repræsenterer de relevante interessenter såsom IKT-industrien, udbydere af elektroniske kommunikationsnet og -tjenester til offentligheden, ***navnlig den europæiske IKT-industri og leverandører, foreninger af små og mellemstore virksomheder,*** forbrugergrupper ***og -foreninger***, akademiske eksperter ***på cybersikkerhedsområdet, de europæiske standardiseringsorganisationer som defineret*** i ***artikel 2, nr. 8), i forordning (EU) nr. 1025/2012, de på dette område relevante EU-agenturer og organer*** og repræsentanter for de kompetente myndigheder, der er givet meddelelse om i henhold til [direktiv om en europæisk

kodeks for elektronisk kommunikation], samt retshåndhævende myndigheder og databeskyttelsestilsynsmyndigheder.

Ændringsforslag 58

Forslag til forordning
Artikel 20 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Embedsperioden for medlemmerne af den stående gruppe af interessenter er to et halvt år. Medlemmer af bestyrelsen kan ikke være medlemmer af den stående gruppe af interessenter. Eksperter fra Kommissionen og medlemsstaterne har ret til at være til stede på møderne og deltage i arbejdet i den stående gruppe af interessenter. Repræsentanter for andre organer, som den administrerende direktør skønner er relevante, og som ikke er medlemmer af den stående gruppe af interessenter, kan indbydes til at være til stede på møderne og deltage i arbejdet i den stående gruppe af interessenter.	4. Embedsperioden for medlemmerne af den stående gruppe af interessenter er to et halvt år. Medlemmer af bestyrelsen ***og forretningsledelsen, bortset fra den administrerende direktør,*** kan ikke være medlemmer af den stående gruppe af interessenter. Eksperter fra Kommissionen og medlemsstaterne har ret til at være til stede på møderne og deltage i arbejdet i den stående gruppe af interessenter. Repræsentanter for andre organer, som den administrerende direktør skønner er relevante, og som ikke er medlemmer af den stående gruppe af interessenter, kan indbydes til at være til stede på møderne og deltage i arbejdet i den stående gruppe af interessenter.

Ændringsforslag 59

Forslag til forordning
Artikel 20 – stk. 5

Kommissionens forslag	*Ændringsforslag*
5. Den stående gruppe af interessenter rådgiver Agenturet med hensyn til udførelsen af dets aktiviteter. Den rådgiver navnlig den administrerende direktør om udarbejdelsen af forslag til Agenturets arbejdsprogram samt om varetagelse af kommunikation med de relevante interessenter om alle spørgsmål, der vedrører arbejdsprogrammet.	5. Den stående gruppe af interessenter rådgiver Agenturet med hensyn til udførelsen af dets aktiviteter. Den rådgiver navnlig den administrerende direktør om udarbejdelsen af forslag til Agenturets arbejdsprogram samt om varetagelse af kommunikation med de relevante interessenter om alle spørgsmål, der vedrører arbejdsprogrammet. ***Den kan også foreslå, at Kommissionen anmoder***

	Agenturet om at forberede forslag til europæiske cybersikkerhedscertificeringsordninger i overensstemmelse med artikel 44, enten på eget initiativ eller efter indgivelse af forslag fra relevante interessenter.

Ændringsforslag 60

Forslag til forordning
Artikel 20 – stk. 5 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	5a. Den stående gruppe af interessenter rådgiver Agenturet med hensyn til forberedelsen af forslag til europæiske cybersikkerhedscertificeringsordninger.

Ændringsforslag 61

Forslag til forordning
Artikel 23 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Agenturet sikrer, at offentligheden og eventuelle interesserede parter får passende, objektive, pålidelige og let tilgængelige oplysninger, især vedrørende resultaterne af dets arbejde. Det offentliggør også interesseerklæringer afgivet i overensstemmelse med artikel 22.	2. Agenturet sikrer, at offentligheden og eventuelle interesserede parter får passende, objektive, pålidelige og let tilgængelige oplysninger, især vedrørende ***drøftelserne og*** resultaterne af dets arbejde. Det offentliggør også interesseerklæringer afgivet i overensstemmelse med artikel 22.

Begrundelse

Gennemsigtighed skal kunne håndhæves under hensyntagen til anvendelse af artikel 24.

Ændringsforslag 62

Forslag til forordning
Artikel 43 – stk. 1

Kommissionens forslag	*Ændringsforslag*
En europæisk cybersikkerhedscertificeringsordning skal attestere, at ***IKT-produkter*** og -tjenester, der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastlagte krav for så vidt angår deres evne til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse ***produkter***, ***processer***, tjenester og systemer.	En europæisk cybersikkerhedscertificeringsordning ***etableres for at styrke sikkerhedsniveauet på det digitale indre marked og anlægge en harmoniseret tilgang på EU-plan til europæisk certificering med henblik på at sikre, at IKT-produkter, -tjenester og -systemer kan stå imod cyberangreb. Ordningen*** skal attestere, at ***IKT-processer, -produkter*** og -tjenester, der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastlagte ***fælles*** krav ***og egenskaber*** for så vidt angår deres evne til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse ***processer***, ***produkter***, tjenester og systemer.

Ændringsforslag 63

Forslag til forordning
Artikel 43 a (ny)

Kommissionens forslag	*Ændringsforslag*
	Artikel 43 a
	Arbejdsprogram
	ENISA skal efter høring af den europæiske cybersikkerhedscertificeringsgruppe og den stående gruppe af interessenter samt efter Kommissionens godkendelse etablere et arbejdsprogram med angivelse af de fælles tiltag, der skal iværksættes på EU-plan med henblik på at sikre en ensartet anvendelse af dette afsnit, og med angivelse af en prioriteret liste over IKT-produkter og -tjenester, for hvilke den anser en europæisk

cybersikkerhedscertificeringsordning at være nødvendig.

Arbejdsprogrammet udarbejdes senest [six months after entry into force of this Regulation] og et nyt arbejdsprogram fastlægges hvert andet år derefter. Arbejdsprogrammet gøres offentligt tilgængeligt.

Ændringsforslag 64

Forslag til forordning
Artikel 44 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. På anmodning fra Kommissionen skal ENISA udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning, som opfylder kravene i denne forordnings artikel 45, 46 og 47. Medlemsstaterne ***eller*** den europæiske cybersikkerhedscertificeringsgruppe ("gruppen"), der er nedsat ved artikel 53, kan foreslå Kommissionen, at der udarbejdes et forslag til en europæisk cybersikkerhedscertificeringsordning.	1. På anmodning fra Kommissionen skal ENISA udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning, som opfylder kravene i denne forordnings artikel 45, 46 og 47. Medlemsstaterne***,*** den europæiske cybersikkerhedscertificeringsgruppe ("gruppen"), der er nedsat ved artikel 53***, eller den stående gruppe af interessenter, der er nedsat ved artikel 20***, kan foreslå Kommissionen, at der udarbejdes et forslag til en europæisk cybersikkerhedscertificeringsordning.

Ændringsforslag 65

Forslag til forordning
Artikel 44 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Under udarbejdelsen af forslaget til den i stk. 1 omhandlede ordning skal ENISA høre alle relevante interessenter ***og samarbejde tæt med gruppen. Gruppen yder ENISA den bistand*** og ***ekspertrådgivning, som ENISA har behov for i forbindelse med*** udarbejdelsen af ***forslaget*** til en ordning***, herunder også udtalelser om nødvendigt***.	2. Under udarbejdelsen af forslaget til den i stk. 1 omhandlede ordning skal ENISA høre ***den stående gruppe af interessenter, navnlig de europæiske standardiseringsorganisationer og*** alle ***andre*** relevante interessenter***, herunder forbrugerorganisationer, gennem en formel, standardiseret og gennemsigtig proces*** og ***samarbejde tæt med gruppen***

	under hensyntagen til allerede eksisterende nationale og internationale standarder. Ved udarbejdelsen af et forslag til en ordning opretter ENISA en tjekliste over risici og tilsvarende cybersikkerhedskarakteristika.
	Gruppen yder ENISA den bistand og ekspertrådgivning, som ENISA har behov for i forbindelse med udarbejdelsen af forslaget til en ordning, herunder også udtalelser om nødvendigt.
	ENISA kan også, hvis det er relevant, nedsætte en interessentekspertgruppe bestående af medlemmer af den stående gruppe af interessenter og andre relevante interessenter med særlig sagkundskab på området for det pågældende forslag til en ordning, med det formål at yde yderligere bistand og rådgivning.

Ændringsforslag 66

Forslag til forordning
Artikel 44 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. ENISA fremsender forslaget til en europæisk cybersikkerhedscertificeringsordning udarbejdet i henhold til stk. 2 til Kommissionen.	3. ENISA fremsender forslaget til en europæisk cybersikkerhedscertificeringsordning udarbejdet i henhold til stk. 2 til Kommissionen***, som vurderer dets egnethed til at nå målene i den stk. 1 omhandlede anmodning.***

Ændringsforslag 67

Forslag til forordning
Artikel 44 – stk. 3 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	3a. ENISA har tavshedspligt om alle oplysninger, det får kendskab til under udførelsen af dets opgaver i henhold til

denne forordning.

Ændringsforslag 68

Forslag til forordning
Artikel 44 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Kommissionen ***kan på grundlag af den af ENISA foreslåede ordning*** vedtage ***gennemførelsesretsakter*** i overensstemmelse med artikel 55***, stk. 1, vedrørende*** europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der opfylder kravene i denne forordnings artikel 45, 46 og 47.	4. Kommissionen ***har beføjelse til at*** vedtage ***delegerede retsakter*** i overensstemmelse med artikel 55***a vedrørende oprettelsen af*** europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der opfylder kravene i denne forordnings artikel 45, 46 og 47. ***Når Kommissionen vedtager disse delegerede retsakter, baserer den cybersikkerhedscertificeringsordningerne for IKT-produkter og -tjenester på relevante forslag til ordninger fremsat af ENISA. Kommissionen kan høre Det Europæiske Databeskyttelsesråd og tage hensyn til dets meninger inden vedtagelsen af sådanne gennemførelsesretsakter.***

Ændringsforslag 69

Forslag til forordning
Artikel 44 – stk. 5

Kommissionens forslag	*Ændringsforslag*
5. ENISA skal drive en dedikeret hjemmeside, der giver oplysninger om og offentlig omtale af de europæiske cybersikkerhedscertificeringsordninger.	5. ENISA skal drive en dedikeret hjemmeside, der giver oplysninger om og offentlig omtale af de europæiske cybersikkerhedscertificeringsordninger***, herunder oplysninger om alle forslag til ordninger, som Kommissionen har anmodet ENISA om at udarbejde***.

Ændringsforslag 70

Forslag til forordning
Artikel 45 – stk. 1 – indledning

Kommissionens forslag	*Ændringsforslag*
En europæisk cybersikkerhedscertificeringsordning skal være udformet således at den***, alt efter relevans,*** tager hensyn til følgende sikkerhedsmål:	***Hver*** europæisk cybersikkerhedscertificeringsordning skal være udformet således***,*** at den ***som minimum*** tager hensyn til følgende sikkerhedsmål***, for så vidt de er relevante***:

Ændringsforslag 71

Forslag til forordning
Artikel 45 – stk. 1 – litra g

Kommissionens forslag	*Ændringsforslag*
g) sikring af, at IKT-produkter og -tjenester er forsynet med ajourført software og ikke indeholder kendte svagheder og har mekanismer til sikker opdatering af software***.***	g) sikring af, at IKT-produkter og -tjenester er forsynet med ajourført software og ***hardware, der*** ikke indeholder kendte svagheder og ***sikring af, at de er udformet og implementeret på en måde, der effektivt begrænser deres modtagelighed for sårbarheder, og sikring af, at de*** har mekanismer til sikker opdatering af software***, herunder opgradering af hardware og automatiske sikkerhedsopdateringer;***

Ændringsforslag 72

Forslag til forordning
Artikel 45 – stk. 1 – litra g a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ga) sikring af, at IKT-produkter og -tjenester udvikles og opereres på en sådan måde, at et højt niveau af cybersikkerhed og databeskyttelse er prækonfigureret i overensstemmelse med princippet om "sikkerhed i designet".

Ændringsforslag 73

Forslag til forordning
Artikel 46 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. ***En*** europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende tillidsniveauer: ***grundlæggende***, ***betydeligt*** og/eller ***højt*** for IKT-produkter og -tjenester, der er certificeret under ordningen.	1. ***Hver*** europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende ***risikobaserede*** tillidsniveauer: ***"funktionelt sikkert", "betydeligt sikkert"*** og/eller ***"særdeles sikkert"*** for IKT-produkter og -tjenester, der er certificeret under ordningen. ***Tillidsniveauet for hvert forslag til en europæisk cybersikkerhedscertificeringsordning skal bestemmes på grundlag af de risici, som er fastlagt i den tjekliste, der er omhandlet i artikel 44, stk. 2, og tilgængeligheden af cybersikkerhedsforanstaltninger til imødegåelse af disse risici i de IKT-produkter og -tjenester, som certificeringsordningen finder anvendelse på.***

Ændringsforslag 74

Forslag til forordning
Artikel 46 – stk. 1 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	1a. De enkelte ordninger skal anføre, hvilken vurderingsmetode eller evalueringsproces der skal følges til udstedelse af attester på de enkelte tillidsniveauer afhængig af den påtænkte anvendelse af og den iboende risiko i IKT-produkterne og -tjenesterne under ordningen.

Ændringsforslag 75

Forslag til forordning
Artikel 46 – stk. 2 – indledning

Kommissionens forslag	*Ændringsforslag*
2. Tillidsniveauerne ***grundlæggende***, ***betydeligt*** og ***højt*** skal opfylde følgende kriterier:	2. Tillidsniveauerne ***"funktionelt sikkert"***, ***"betydeligt sikkert"*** og ***"særdeles sikkert"*** skal ***henholdsvis*** opfylde følgende kriterier:

Ændringsforslag 76

Forslag til forordning
Artikel 46 – stk. 2 – litra a

Kommissionens forslag	*Ændringsforslag*
a) tillidsniveauet ***"grundlæggende"*** henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en ***begrænset*** grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for ***et IKT-produkt*** eller ***en IKT-tjeneste***, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for cybersikkerhedshændelser	a) tillidsniveauet ***"funktionelt sikkert"*** henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en ***tilstrækkelig*** grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for ***IKT-processen, -produktet*** eller ***-tjenesten***, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for cybersikkerhedshændelser

Ændringsforslag 77

Forslag til forordning
Artikel 46 – stk. 2 – litra b

Kommissionens forslag	*Ændringsforslag*
b) tillidsniveauet ***"betydeligt"*** henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en betydelig grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for ***et IKT-produkt*** eller ***en IKT-tjeneste***, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil	b) tillidsniveauet ***"betydeligt sikkert"*** henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en betydelig grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for ***IKT-processen, -produktet*** eller ***IKT-tjenesten***, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og

knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for cybersikkerhedshændelser betydeligt	hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for cybersikkerhedshændelser betydeligt

Ændringsforslag 78

Forslag til forordning
Artikel 46 – stk. 2 – litra c

Kommissionens forslag	*Ændringsforslag*
c) tillidsniveauet ***"højt"*** henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en større grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for ***et IKT-produkt*** eller ***en IKT-tjeneste*** end attester med niveauet ***"betydelig"***, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at forhindre cybersikkerhedshændelser.	c) tillidsniveauet ***"særdeles sikkert"*** henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en større grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for ***IKT-processen, -produktet*** eller ***-tjenesten*** end attester med niveauet ***"betydeligt sikkert"***, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at forhindre cybersikkerhedshændelser. ***Dette gælder især for produkter og tjenester, der er beregnet til brug for operatører af væsentlige tjenester som defineret i artikel 4, nr. 4), i direktiv 2016/1148/EU.***

Ændringsforslag 79

Forslag til forordning
Artikel 47 – stk. 1 – indledning

Kommissionens forslag	*Ændringsforslag*
1. ***En europæisk*** cybersikkerhedscertificeringsordning skal omfatte følgende elementer:	1. ***Hver europæisk*** cybersikkerhedscertificeringsordning skal ***som minimum*** omfatte følgende elementer***, hvis det er relevant***:

Ændringsforslag 80

Forslag til forordning
Artikel 47 – stk. 1 – litra a

Kommissionens forslag	*Ændringsforslag*
a) ***certificeringens*** genstand og omfang, herunder typer eller kategorier af IKT-produkter og -tjenester, der er omfattet	a) ***certificeringsordningens*** genstand og omfang, herunder ***specifikke sektorer, der er omfattet, og*** typer eller kategorier af IKT-produkter og -tjenester, der er omfattet

Ændringsforslag 81

Forslag til forordning
Artikel 47 – stk. 1 – litra b

Kommissionens forslag	*Ændringsforslag*
b) detaljeret specifikation af cybersikkerhedskravene, som de specifikke IKT-produkter og -tjenester evalueres i forhold til, ***f.eks.*** ved at henvise til ***europæiske*** eller internationale standarder eller tekniske specifikationer	b) detaljeret specifikation af cybersikkerhedskravene, som de specifikke IKT-produkter og -tjenester evalueres i forhold til, ***navnlig*** ved at henvise til internationale, ***europæiske*** eller ***nationale*** standarder eller tekniske specifikationer

Ændringsforslag 82

Forslag til forordning
Artikel 47 – stk. 1 – litra b a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ba) detaljeret specifikation af, om en udstedt certificering kun kan gælde for et enkelt produkt eller for et helt produktsortiment, f.eks. forskellige versioner eller modeller af det samme basisprodukt

Ændringsforslag 83

Forslag til forordning
Artikel 47 – stk. 1 – litra c a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ca) angivelse af, hvorvidt egenerklæring om overensstemmelse er tilladt i henhold til ordningen, og den gældende procedure for overensstemmelsesvurdering eller egenerklæring om overensstemmelse eller begge;

Ændringsforslag 84

Forslag til forordning
Artikel 47 – stk. 1 – litra c b (nyt)

Kommissionens forslag	*Ændringsforslag*
	cb) certificeringskrav, der defineres på en sådan måde, at certificeringen kan indarbejdes i eller baseres på producentens systematiske cybersikkerhedsprocesser, som efterleves i hele det tidsrum, hvor IKT-processen, -produktet eller -tjenesten udformes og udvikles samt i dens/dets livscyklus

Ændringsforslag 85

Forslag til forordning
Artikel 47 – stk. 1 – litra f

Kommissionens forslag	*Ændringsforslag*
f) hvis ordningen fastsætter mærker eller etiketter, omstændighederne under hvilke disse mærker eller etiketter kan anvendes	f) hvis ordningen fastsætter mærker eller etiketter, ***f.eks. et EU-mærke for cybersikkerhedsoverensstemmelse, der betyder, at IKT-processen, -produktet eller -tjenesten overholder kriterierne i ordningen,*** omstændighederne under hvilke disse mærker eller etiketter kan anvendes

Ændringsforslag 86

Forslag til forordning
Artikel 47 – stk. 1 – litra g

Kommissionens forslag	*Ændringsforslag*
g) ***hvis overvågningen er en del af ordningen, reglerne*** for overvågning af overensstemmelsen med attesternes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav	g) ***reglerne*** for overvågning af overensstemmelsen med attesternes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav***, herunder - hvis det er relevant og muligt - obligatoriske opdateringer, opgraderinger eller patches til den/det pågældende IKT-proces, -produkt eller -tjeneste***

Ændringsforslag 87

Forslag til forordning
Artikel 47 – stk. 1 – litra h

Kommissionens forslag	*Ændringsforslag*
h) betingelserne for udstedelse, bibeholdelse, forlængelse, udvidelse og indskrænkning af certificeringens omfang	h) betingelserne for udstedelse, bibeholdelse, forlængelse, ***fornyelse,*** udvidelse og indskrænkning af certificeringens omfang

Ændringsforslag 88

Forslag til forordning
Artikel 47 – stk. 1 – litra i

Kommissionens forslag	*Ændringsforslag*
i) regler om følgerne af certificerede IKT-produkters og -tjenesters manglende overholdelse af certificeringskravene	i) regler om følgerne af certificerede IKT-produkters og -tjenesters manglende overholdelse af certificeringskravene ***og generelle oplysninger om de i denne forordnings artikel 54 fastlagte sanktioner***

Ændringsforslag 89

Forslag til forordning
Artikel 47 – stk. 1 – litra j

Kommissionens forslag	*Ændringsforslag*
j) regler om, hvordan hidtil uopdagede cybersikkerhedssårbarheder i IKT-produkter og -tjenester skal indberettes og håndteres	j) regler om, hvordan hidtil uopdagede cybersikkerhedssårbarheder i IKT-produkter og -tjenester skal indberettes og håndteres***, herunder gennem politikker for koordineret formidling af sårbarheder***

Ændringsforslag 90

Forslag til forordning
Artikel 47 – stk. 1 – litra l

Kommissionens forslag	*Ændringsforslag*
l) angivelse af nationale cybersikkerhedscertificeringsordninger, som dækker samme typer eller kategori af IKT-produkter og -tjenester	l) angivelse af nationale ***eller internationale*** cybersikkerhedscertificeringsordninger ***eller eksisterende internationale aftaler om gensidig anerkendelse***, som dækker samme typer eller kategori af IKT-produkter og -tjenester

Ændringsforslag 91

Forslag til forordning
Artikel 47 – stk. 1 – litra m a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ma) attesters maksimale gyldighedsperiode

Ændringsforslag 92

Forslag til forordning
Artikel 47 – stk. 1 – litra m b (nyt)

Kommissionens forslag	*Ændringsforslag*
	mb) regler om afprøvning af modstandsdygtigheden på tillidsniveauet "særdeles sikker"

Ændringsforslag 93

Forslag til forordning
Artikel 47 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Hvis det er fastsat i en EU-retsakt, kan certificering i henhold til en europæisk cybersikkerhedscertificeringsordning anvendes til at påvise formodning om overensstemmelse med den pågældende retsakt.	3. Hvis det er fastsat i en ***fremtidig*** EU-retsakt, kan certificering i henhold til en europæisk cybersikkerhedscertificeringsordning anvendes til at påvise formodning om overensstemmelse med den pågældende retsakt.

Ændringsforslag 94

Forslag til forordning
Artikel 48 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. ***Certificeringen*** skal være frivillig, medmindre andet er fastsat i EU-retten.	2. ***Certificering i henhold til en europæisk cybersikkerhedscertificeringsordning skal være obligatorisk for IKT-produkter og -tjenester med en høj iboende risiko, som specifikt er beregnet til brug for operatører af væsentlige tjenester som defineret i artikel 4, nr. 4, i direktiv 2016/1148/EU. For alle andre IKT-produkter og -tjenester*** skal ***certificeringen*** være frivillig, medmindre andet er fastsat i EU-retten.

Ændringsforslag 95

Forslag til forordning
Artikel 48 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. ***En europæisk cybersikkerhedsattest*** i medfør af denne artikel skal udstedes af de	3. ***Europæiske cybersikkerhedsattester*** i medfør af denne artikel skal udstedes af de

overensstemmelsesvurderingsorganer, der er omhandlet i artikel 51, på grundlag af de kriterier, der fremgår af den europæiske cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 44.

overensstemmelsesvurderingsorganer, der er omhandlet i artikel 51, på grundlag af de kriterier, der fremgår af den europæiske cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 44.

Som alternativ til certificering udstedt af overensstemmelsesvurderingsorganer kan producenter og tjenesteudbydere, hvis der i den pågældende ordning er fastsat en sådan mulighed, fremsætte en egenerklæring om overensstemmelse, hvori de erklærer, at en proces, et produkt eller en tjeneste overholder kriterierne i certificeringsordningen. I sådanne tilfælde skal producenten eller tjenesteyderen efter anmodning udlevere egenerklæringen om overensstemmelse til den anmodende nationale certificeringstilsynsmyndighed og ENISA.

Ændringsforslag 96

Forslag til forordning
Artikel 48 – stk. 4 – indledning

Kommissionens forslag	*Ændringsforslag*
4. Som en undtagelse fra stk. 3 kan det i behørigt begrundede tilfælde fastsættes i en europæisk cybersikkerhedscertificeringsordning, at en europæisk cybersikkerhedsattest, der fremgår af denne ordning, kun kan udstedes af et offentligt organ. Et sådant offentligt organ skal være en af følgende:	4. Som en undtagelse fra stk. 3 kan det i behørigt begrundede tilfælde ***såsom hensyntagen den til nationale sikkerhed*** fastsættes i en europæisk cybersikkerhedscertificeringsordning, at en europæisk cybersikkerhedsattest, der fremgår af denne ordning, kun kan udstedes af et offentligt organ. Et sådant offentligt organ skal være en af følgende:

Ændringsforslag 97

Forslag til forordning
Artikel 48 – stk. 5

Kommissionens forslag	*Ændringsforslag*
5. Den fysiske eller juridiske person, der indgiver sine IKT-produkter og -	5. Den fysiske eller juridiske person, der indgiver sine IKT-produkter og -

tjenester til certificeringsmekanismen, skal fremlægge alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, for det i artikel 51 omhandlede overensstemmelsesvurderingsorgan.	tjenester til certificeringsmekanismen, skal fremlægge alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, for det i artikel 51 omhandlede overensstemmelsesvurderingsorgan***, herunder oplysninger om eventuelle sikkerhedssårbarheder***.

Ændringsforslag 98

Forslag til forordning
Artikel 48 – stk. 6

Kommissionens forslag	*Ændringsforslag*
6. Attester udstedes for ***en*** periode ***på højst tre år*** og kan forlænges på samme betingelser, såfremt ***de relevante*** krav fortsat er opfyldt.	6. Attester udstedes for ***og er gyldige i den maksimale*** periode***, som er fastsat i den enkelte certificeringsordning,*** og kan forlænges på samme betingelser, såfremt ***kravene i ordningen, herunder eventuelle reviderede eller ændrede*** krav***,*** fortsat er opfyldt.

Ændringsforslag 99

Forslag til forordning
Artikel 48 – stk. 6 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	6a. Attester er gyldige for alle nye versioner af en proces, et produkt eller en tjeneste, såfremt den primære årsag til den nye version er et patch, et fix eller en anden løsning på kendte eller potentielle sikkerhedssårbarheder eller -trusler.

Ændringsforslag 100

Forslag til forordning
Artikel 49 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, skal ophøre med at have virkning fra det tidspunkt, der fastsættes i den ***gennemførelsesretsakt***, som vedtages i medfør af artikel 44, stk. 4, jf. dog nærværende artikels stk. 3. Bestående nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter og -tjenester, der ikke er omfattet af en europæisk cybersikkerhedscertificeringsordning, fortsætter med at bestå.	1. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, skal ophøre med at have virkning fra det tidspunkt, der fastsættes i den ***delegerede retsakt***, som vedtages i medfør af artikel 44, stk. 4, jf. dog nærværende artikels stk. 3***. Kommissionen overvåger overholdelsen af dette afsnit for at undgå parallelle ordninger.*** Bestående nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter og -tjenester, der ikke er omfattet af en europæisk cybersikkerhedscertificeringsordning, fortsætter med at bestå.

Ændringsforslag 101

Forslag til forordning
Artikel 49 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Eksisterende attester udstedt i henhold til en national cybersikkerhedscertificeringsordning forbliver gyldige indtil deres udløbsdato.	3. Eksisterende attester udstedt i henhold til en national cybersikkerhedscertificeringsordning ***og dækket af en europæisk cybersikkerhedscertificeringsordning*** forbliver gyldige indtil deres udløbsdato.

Ændringsforslag 102

Forslag til forordning
Artikel 50 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Hver national certificeringstilsynsmyndighed skal med hensyn til dens organisation,	3. Hver national certificeringstilsynsmyndighed skal med hensyn til dens organisation,

finansieringsbeslutninger, retlige struktur og beslutningstagning være uafhængig af de enheder, som den fører tilsyn med.	finansieringsbeslutninger, retlige struktur og beslutningstagning være uafhængig af de enheder, som den fører tilsyn med***, og må ikke være et overensstemmelsesvurderingsorgan eller et nationalt akkrediteringsorgan***.

Ændringsforslag 103

Forslag til forordning
Artikel 50 – stk. 6 – litra a

Kommissionens forslag	*Ændringsforslag*
a) overvåge og håndhæve anvendelsen af bestemmelserne i dette afsnit på nationalt niveau og føre tilsyn med***, at de attester, der er udstedt af overensstemmelsesvurderingsorganer***, ***som*** er ***etableret på deres respektive område, er*** i ***overensstemmelse med de krav***, ***der er fastsat i dette afsnit og i den tilsvarende europæiske cybersikkerhedscertificeringsordning***	a) overvåge og håndhæve anvendelsen af bestemmelserne i dette afsnit på nationalt niveau og føre tilsyn med ***overholdelsen - i overensstemmelse med reglerne, der er vedtaget af den europæiske cybersikkerhedscertificeringsgruppe i henhold til artikel 53, stk. 3, litra da) - af:*** ***i) de attester, der er udstedt af overensstemmelsesvurderingsorganer, som er etableret på deres respektive område, med de krav, der er fastsat i dette afsnit og i den tilsvarende europæiske cybersikkerhedscertificeringsordning og*** ***ii) egenerklæringer om overensstemmelse, som er afgivet i henhold til en ordning for en IKT- proces, et IKT-produkt eller en IKT-tjeneste***

Ændringsforslag 104

Forslag til forordning
Artikel 50 – stk. 6 – litra b

Kommissionens forslag	*Ændringsforslag*
b) overvåge ***og*** føre tilsyn med overensstemmelsesvurderingsorganers aktiviteter i forbindelse med denne forordning, herunder med hensyn til anmeldelsen af	b) overvåge***,*** føre tilsyn med ***og mindst hvert andet år vurdere*** overensstemmelsesvurderingsorganers aktiviteter i forbindelse med denne forordning, herunder med hensyn til

overensstemmelsesvurderingsorganer og de relaterede opgaver, der er fastsat i denne forordnings artikel 52	anmeldelsen af overensstemmelsesvurderingsorganer og de relaterede opgaver, der er fastsat i denne forordnings artikel 52

Ændringsforslag 105

Forslag til forordning
Artikel 50 – stk. 6 – litra c

Kommissionens forslag	*Ændringsforslag*
c) behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist	c) behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, ***eller i forbindelse med afgivne egenerklæringer om overensstemmelse,*** undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist

Ændringsforslag 106

Forslag til forordning
Artikel 50 – stk. 6 – litra c a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ca) rapportere resultaterne af kontrollen under litra a) og vurderingerne under litra b) til ENISA og den europæiske cybersikkerhedscertificeringsgruppe

Ændringsforslag 107

Forslag til forordning
Artikel 50 – stk. 6 – litra d

Kommissionens forslag	*Ændringsforslag*
d) samarbejde med andre nationale	d) samarbejde med andre nationale

certificeringstilsynsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings eller specifikke cybersikkerhedscertificeringsordningers krav	certificeringstilsynsmyndigheder***,*** ***nationale akkrediteringsorganer*** eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings eller specifikke cybersikkerhedscertificeringsordningers krav***, herunder vildledende, falske eller svigagtige påstande om certificering***

Ændringsforslag 108

Forslag til forordning
Artikel 50 – stk. 7 – litra c a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ca) at kunne inddrage akkrediteringen af overensstemmelsesvurderingsorganer, som ikke overholder bestemmelserne i denne forordning.

Ændringsforslag 109

Forslag til forordning
Artikel 50 – stk. 7 – litra e

Kommissionens forslag	*Ændringsforslag*
e) at kunne tilbagekalde, i overensstemmelse med national ret, attester, som ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning	e) at kunne tilbagekalde, i overensstemmelse med national ret, attester, som ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning ***og underrette de nationale akkrediteringsorganer herom***

Ændringsforslag 110

Forslag til forordning
Artikel 50 – stk. 7 – litra f a (nyt)

Kommissionens forslag	*Ændringsforslag*
	fa) at kunne foreslå ENISA-eksperter som deltagere i interessentekspertgruppen som omhandlet i artikel 44, stk. 2

Ændringsforslag 111

Forslag til forordning
Artikel 50 – stk. 8 – afsnit 1 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	Kommissionen stiller et generelt elektronisk informationsstøttesystem til rådighed med henblik på denne udveksling.

Ændringsforslag 112

Forslag til forordning
Artikel 50 a (ny)

Kommissionens forslag	*Ændringsforslag*
	Artikel 50 a
	Fagfællebedømmelse
	1. De nationale certificeringstilsynsmyndigheder skal underkastes en fagfællebedømmelse i forbindelse med enhver aktivitet, som de udfører i henhold til artikel 50 i denne forordning.
	2. Fagfællebedømmelse skal omfatte vurderinger af de procedurer, der er indført af de nationale certificeringsmyndigheder, især procedurerne, der kontrollerer overholdelsen for de produkter, der er omfattet af cybersikkerhedscertificering, personalets kompetencer, korrektheden af kontrolundersøgelserne og inspektionsmetoden og korrektheden af resultaterne. Ved fagfællebedømmelsen

skal det også vurderes, hvorvidt de pågældende nationale certificeringstilsynsmyndigheder har tilstrækkelige ressourcer til, at de kan udføre deres opgaver i overensstemmelse med artikel 50, stk. 4.

3. Fagfællebedømmelse af en national certificeringstilsynsmyndighed skal foretages af to nationale certificeringstilsynsmyndigheder fra andre medlemsstater og Kommissionen, og den skal gennemføres mindst en gang hvert femte år. ENISA kan deltage i fagfællebedømmelsen og træffer afgørelse om dets deltagelse på baggrund af en risikovurderingsanalyse.

4. Kommissionen har beføjelse til i henhold til artikel 55a at vedtage delegerede retsakter med henblik på udarbejdelse af en plan for fagfællebedømmelserne, der omfatter en periode på mindst fem år, og som fastsætter kriterier for sammensætningen af fagfællebedømmelsesteamet, den anvendte metode for bedømmelsen, tidsplanen, hyppigheden og de andre opgaver i forbindelse med fagfællebedømmelsen. Ved vedtagelsen af disse delegerede retsakter tager Kommissionen hensyn til gruppens betragtninger.

5. Resultaterne af fagfællebedømmelsen gennemgås af gruppen. ENISA udarbejder et referat af resultaterne og offentliggør det.

Ændringsforslag 113

Forslag til forordning
Artikel 51 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. Hvis producenterne vælger "egenerklæring om overensstemmelse" i henhold til artikel 48, stk. 3, tager

	overensstemmelsesvurderingsorganerne yderligere skridt med henblik på at kontrollere de interne procedurer, som producenterne har fulgt, så det sikres, at deres produkter og/eller tjenester overholder kravene i den europæiske cybersikkerhedscertificeringsordning.

Ændringsforslag 114

Forslag til forordning
Artikel 53 – stk. 3 – litra d a (nyt)

Kommissionens forslag	*Ændringsforslag*
	da) at vedtage bindende regler for fastsættelse af de intervaller, hvormed de nationale certificeringstilsynsmyndigheder skal foretage kontrol af attester og egenerklæringer om overensstemmelse, og vedtage kriterier, omfang og formål med disse kontroller samt vedtage fælles regler og standarder for rapportering i henhold til artikel 50, stk. 6

Ændringsforslag 115

Forslag til forordning
Artikel 53 – stk. 3 – litra e

Kommissionens forslag	*Ændringsforslag*
e) at undersøge de relevante udviklinger inden for cybersikkerhedscertificering og udveksle god praksis om cybersikkerhedscertificeringsordninger	e) at undersøge de relevante udviklinger inden for cybersikkerhedscertificering og udveksle ***oplysninger og*** god praksis om cybersikkerhedscertificeringsordninger

Ændringsforslag 116

Forslag til forordning
Artikel 53 – stk. 3 – litra f a (nyt)

Kommissionens forslag	*Ændringsforslag*
	fa) at udveksle bedste praksis med hensyn til efterforskning af overensstemmelsesvurderingsorganer, indehavere af europæiske cybersikkerhedsattester og producenter og tjenesteudbydere, der har afgivet egenerklæringer om overensstemmelse;

Ændringsforslag 117

Forslag til forordning
Artikel 53 – stk. 3 – litra f b (nyt)

Kommissionens forslag	*Ændringsforslag*
	fb) at lette tilpasningen af de europæiske cybersikkerhedscertificeringsordninger til internationalt anerkendte standarder og, hvor det er relevant, anbefale ENISA områder, hvor ENISA bør samarbejde med relevante internationale og europæiske standardiseringsorganisationer for at afhjælpe mangler eller huller i internationalt anerkendte standarder;

Ændringsforslag 118

Forslag til forordning
Artikel 53 – stk. 3 – litra f c (nyt)

Kommissionens forslag	*Ændringsforslag*
	fc) at rådgive ENISA, når det i artikel 43 nævnte arbejdsprogram udarbejdes, om oprettelsen af en prioriteret liste over IKT-produkter og - tjenester, for hvilke den mener, der er behov for en europæisk cybersikkerhedscertificeringsordning

Ændringsforslag 119

Forslag til forordning
Artikel 53 – stk. 4 – afsnit 1 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ENISA sikrer, at dagsordenen, referaterne og de trufne beslutninger registreres, og at de offentliggjorte versioner af disse dokumenter gøres tilgængelige for offentligheden på ENISA's webside efter hvert møde i gruppen.

Ændringsforslag 120

Forslag til forordning
Artikel 55 a (ny)

Kommissionens forslag	*Ændringsforslag*
	Artikel 55a
	Udøvelse af de delegerede beføjelser
	Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.
	Beføjelsen til at vedtage delegerede retsakter i henhold til artikel 44, stk. 4, og artikel 50a, stk. 4, tillægges Kommissionen i en periode på fem år fra [date of entry into force of the basic legislative act]. Kommissionen udarbejder en rapport vedrørende de delegerede beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.
	Den i artikel 44, stk. 4, og artikel 50a, stk. 4, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om

tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af de delegerede retsakter, der allerede er i kraft.

Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016.

Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

En delegeret retsakt vedtaget i henhold til artikel 44, stk. 4, eller artikel 50a, stk. 4, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på [two months] fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med [two months] på Europa-Parlamentets eller Rådets initiativ.

PROCEDURE I RÅDGIVENDE UDVALG

Titel	Forordning om ENISA, EU's Agentur for Cybersikkerhed, om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed").
Referencer	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Korresponderende udvalg Dato for meddelelse på plenarmødet	ITRE 23.10.2017
Udtalelse fra Dato for meddelelse på plenarmødet	IMCO 23.10.2017
Associerede udvalg - dato for meddelelse på plenarmødet	18.1.2018
Ordfører for udtalelse Dato for valg	Nicola Danti 25.9.2017
Behandling i udvalg	21.2.2018 21.3.2018
Dato for vedtagelse	17.5.2018
Resultat af den endelige afstemning	+: 31 –: 2 0: 1
Til stede ved den endelige afstemning - medlemmer	John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Dennis de Jong, Pascal Durand, Evelyne Gebhardt, Robert Jarosław Iwaszkiewicz, Liisa Jaakonsaari, Marlene Mizzi, Nosheena Mobarik, Jiří Pospíšil, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Ivan Štefanec, Catherine Stihler, Mylène Troszczynski, Mihai Ţurcanu, Anneleen Van Bossuyt, Marco Zullo
Til stede ved den endelige afstemning – stedfortrædere	Jan Philipp Albrecht, Kaja Kallas, Arndt Kohn, Emma McClarkin, Adam Szejnfeld, Marc Tarabella, Lambert van Nistelrooij, Kerstin Westphal
Til stede ved den endelige afstemning – stedfortrædere (forretningsordenens art. 200, stk. 2)	Inés Ayala Sender, Flavio Zanonato

ENDELIG AFSTEMNING VED NAVNEOPRÅB I RÅDGIVENDE UDVAG

31	+
ALDE	Dita Charanzová, Kaja Kallas, Jasenko Selimovic
ECR	Daniel Dalton, Emma McClarkin, Nosheena Mobarik, Anneleen Van Bossuyt
EFDD	Marco Zullo
GUE/NGL	Dennis de Jong
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Mihai Ţurcanu, Lambert van Nistelrooij
S&D	Inés Ayala Sender, Nicola Danti, Evelyne Gebhardt, Liisa Jaakonsaari, Arndt Kohn, Marlene Mizzi, Olga Sehnalová, Catherine Stihler, Marc Tarabella, Kerstin Westphal, Flavio Zanonato
Verts/ALE	Jan Philipp Albrecht, Pascal Durand

2	-
EFDD	John Stuart Agnew, Robert Jarosław Iwaszkiewicz

1	0
ENF	Mylène Troszczynski

Symbolforklaring:
+ : for
- : imod
0 : undlod at stemme