



Rådet for
Den Europæiske Union

Bruxelles, den 2. december 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

RESULTAT AF DRØFTELSENE

fra:	Generalsekretariatet for Rådet
dato:	2. december 2020
til:	delegationerne

Vedr.:	Rådets konklusioner om cybersikkerheden ved forbundet udstyr - Rådets konklusioner, som blev godkendt ved skriftlig procedure
--------	--

Vedlagt følger til delegationerne Rådets konklusioner om cybersikkerhed for netforbundne enheder som godkendt af Rådet ved skriftlig procedure den 2. december 2020.

Rådets konklusioner om cybersikkerheden ved forbundet udstyr

Rådet for Den Europæiske Union,

SOM MINDER OM

- Rådets konklusioner om den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU
 - Rådets konklusioner om opbygning af cybersikkerhedskapacitet i EU
 - Rådets konklusioner om betydningen af 5G for den europæiske økonomi og behovet for at afbøde de sikkerhedsrisici, der er forbundet med 5G
 - Rådets konklusioner om fremtiden for et højdigitaliseret Europa efter 2020: "Styrke den digitale og økonomiske konkurrenceevne i hele Unionen og den digitale samhørighed"
 - Rådets konklusioner – Europas digitale fremtid i støbeskeen
 - Det Europæiske Råds konklusioner om covid-19, det indre marked, industripolitik og det digitale og om eksterne forbindelser
 - Europa-Kommissionens meddelelse "Europas digitale fremtid i støbeskeen",
1. **FREMHÆVER**, at Den Europæiske Union og dens medlemsstater skal sikre deres digitale suverænitet og strategiske autonomi, samtidig med at de fastholder en åben økonomi. Dette indebærer styrkelse af evnen til at træffe selvstændige teknologiske valg og, som en af de vigtigste søjler, robuste og sikre infrastrukturer, produkter og tjenester, der kan opbygge tillid til det digitale indre marked og internt i det europæiske samfund. Den Europæiske Unions kerneværdier værner om navnlig privatlivets fred, sikkerheden, ligheden, den menneskelige værdighed, retsstatsprincippet og et åbent internet som forudsætninger for at opnå et samfund, en økonomi og en industri, der er digitalt drevet og sætter mennesket i centrum;

2. **ANERKENDER** den stigende betydning af forbundet udstyr og dets sikkerhed, herunder de maskiner, sensorer og netværk, der udgør tingenes internet (IoT). Forbundet udstyr vil spille en central rolle så vel i den videre udformning af Europas digitale fremtid, set ud fra et industrielt og erhvervsmæssigt synspunkt, som i dagligdagen for forbrugerne af en ny generation af teknologi. Ud over 5G kan kunstig intelligens, kvantecomputing, højtydende databehandling, cloud computing, distributed ledger-teknologier, dvs. blockchain, og alle andre nye applikationer og muligheder for en bæredygtig økonomisk vækst og et højere digitaliseringsniveau i vores samfund kun opnås med cybersikkert forbundet udstyr;
3. **BEMÆRKER**, at den øgede brug af forbrugerprodukter og industrielt internetforbundet udstyr også vil medføre nye risici for privatlivets fred og informations- og cybersikkerheden, herunder i stigende grad potentielle konsekvenser for produkters og datas integritet og tilgængelighed, som kan påvirke sikkerheden direkte. Det er afgørende at minimere sådanne risici af hensyn til beskyttelsen af forbrugerne, styrkelsen af Europas samlede cyberrobusthed og styrkelsen af borgernes tillid til digitale løsninger og teknologier. Dette vil også fremme konkurrenceevnen og innovationskapaciteten hos europæiske udbydere af sådant udstyr. Cybersikkerhed og privatlivets fred bør anerkendes som væsentlige krav i produktinnovation, produktions- og udviklingsprocesser, herunder i designfasen (security by design), og bør sikres gennem hele produktets livscyklus og i hele dets forsyningskæde;
4. **UNDERSTREGER**, at det ud over at sikre et højt sikkerhedsniveau for forbundet udstyr er lige så vigtigt at øge forbrugernes bevidsthed om dets potentielle risici for privatlivets fred og sikkerheden. Dette vil bidrage til at minimere risiciene ved en øget brug af forbundet udstyr, styrke tilliden til det digitale indre marked og maksimere udbyttet af de økonomiske og samfundsmæssige fordele, som teknologier med forbundet udstyr medfører;

5. UNDERSTREGER, at så vel offentlige investeringer i forskning og innovation, navnlig gennem Horisont Europa og programmet for et digitalt Europa, som private investeringer kan skabe værdifulde incitamenters til at gøre forbundet udstyr mere sikkert og trygt og dermed intelligente kommunikationsnetværk mere robuste. Investeringer i den nødvendige digitale infrastruktur og teknologi til udbredelse af de nyeste teknologier med forbundet udstyr bør også fremskyndes for at opnå industrielt og digitalt lederskab og for at sikre strategisk autonomi, samtidig med at den åbne økonomi fastholdes;
6. UNDERSTREGER behovet for at sikre en høj grad af komplementaritet og sammenlignelighed mellem IKT-systemernes og IKT-komponenternes sikkerhedsfunktioner, som anvendes i mange forskellige sektorer på det digitale indre marked;
7. ANERKENDER den nuværende udvikling på EU-plan, der skal øge cybersikkerheden ved forbundet udstyr, navnlig nylige initiativer fra Kommissionens side til på kort sigt at tackle cybersikkerhedsaspekter i relevante retsakter, f.eks. retsakter som led i den nye lovgivningsmæssige ramme, særlig direktiv 2014/53/EU (radioudstyrsdirektivet); UNDERSTREGER betydningen på lang sigt af en vurdering af behovet for horisontal lovgivning, der også præciserer de nødvendige betingelser for omsætning, for at tackle alle relevante aspekter af cybersikkerheden ved forbundet udstyr, såsom tilgængelighed, integritet og fortrolighed; HILSER i denne forbindelse en drøftelse med henblik på at undersøge anvendelsesområdet for denne lovgivning og dens forbindelser med rammen for cybersikkerhedscertificering som defineret i forordningen om cybersikkerhed VELKOMMEN med henblik på at højne sikkerhedsniveauet på det digitale indre marked;
8. UNDERSTREGER, at cybersikkerhedskrav for at undgå tvetydighed og fragmentering i lovgivningen bør fastsættes i overensstemmelse med relevant EU-lovgivning, herunder forordningen om cybersikkerhed, den nye lovgivningsmæssige ramme, forordningen om europæisk standardisering og eventuel fremtidig horisontal lovgivning;

9. ANERKENDER den vigtige rolle, som alle interessenter, navnlig producenterne, spiller for at øge cybersikkerheden ved forbundet udstyr i det indre marked og OPFORDRER derfor TIL koordinering og tæt samarbejde med alle relevante offentlige og private interessenter, også med henblik på eventuel fremtidig lovgivning;
- 9a. SER med tilfredshed PÅ det af ENISA ledede igangværende arbejde med at udarbejde udkast til de første EU-cybersikkerhedscertificeringsordninger, nemlig de foreslåede fælles EU-kriterier og de foreslåede ordninger for cloudtjenester. Disse ordninger vil udgøre det relevante fundament for certificering af forbundet udstyr;
10. FREMHÆVER, at en eventuel supplerende certificeringsordning for forbundet udstyr og relaterede tjenester, som måtte blive fastlagt i Unionens rullende arbejdsprogram og defineret i forordningen om cybersikkerhed, bør præcisere, hvordan de gældende sikkerhedskrav på det relevante sikringsniveau bør opfyldes på grundlag af specifikke europæiske og internationalt anerkendte standarder, uanset hvilken sektor produktet skal anvendes i, og hvilke testspecifikationer, certifikater osv. der skal anvendes;
11. ANERKENDER, at certificering af forbundet udstyr vil kræve relevante normer, standarder eller tekniske specifikationer med henblik på cybersikkerhedsevalueringer i henhold til forordningen om cybersikkerhed; FREMHÆVER derfor behovet for at indføre normer, standarder eller tekniske specifikationer for cybersikkerheden ved forbundet udstyr og HENSTILLER, at den europæiske standardiseringsorganisations indsats i denne sammenhæng intensiveres; NOTERER SIG samtidig ETSI's cybersikkerhedsstandard EN 303 645 for IoT-udstyr for forbrugere som et vigtigt skridt i denne retning;

12. OPFORDRER Kommissionen TIL at overveje en anmodning om kandidater til cybersikkerhedscertificeringsordninger for forbundet udstyr og relaterede tjenester baseret på Unionens rullende arbejdsprogram, der er under udarbejdelse, under nøje hensyntagen til de horisontale europæiske cybersikkerhedscertificeringsordninger, der i øjeblikket er under udvikling. En sådan ordning vil på frivilligt grundlag gøre det muligt for producenterne af disse produkter at promovere produkter med det vurderede sikringsniveau;
13. OPFORDRER TIL en drøftelse om, hvordan målet om cybersikkerhed kan forankres i fremtidig horisontal lovgivning, der omfatter cybersikkerhedsrisici ved forbundet udstyr, og NOTERER SIG samtidig behovet for, hvor dette er relevant, at overveje en tilpasning af væsentlige krav i de respektive direktiver i den nye lovgivningsmæssige ramme;
14. OPFORDRER Kommissionen TIL om fornødent også at overveje supplerende sektorspecifikke forordninger, der bør definere, hvilket cybersikkerhedsniveau der bør opfyldes af det forbundne udstyr, for at sikre, at der indføres specifikke krav til sikkerhed og beskyttelse af privatlivets fred for udstyr med større sikkerhedsrisici;
15. UNDERSTREGER behovet for at forbedre de europæiske borgeres livskvalitet og trivsel og fremme tilliden til det digitale indre marked. Sikkerheden og privatlivets fred i vores samfund er afgørende for at bevare vores kerneværdier i Unionen; UNDERSTREGER derfor behovet for at bygge videre på den ramme, som er fastlagt i forordningen om cybersikkerhed til harmonisering af sikkerhedskravene i henhold til forskellige sikringsniveauer i alle sektorer inden for den nye lovgivningsmæssige ramme, for at undgå fragmentering og dobbeltkontrol af identiske krav og skabe lige vilkår for konkurrence og innovation i hele Den Europæiske Union;

16. OPFORDRER Kommissionen, EU's Agentur for Cybersikkerhed (ENISA), Udvalget for Overensstemmelsesvurdering og Markedstilsyn på Teleområdet og Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG) TIL aktivt at deltage i dette initiativ til styrkelse af det digitale indre marked og tilliden til IKT-produkter, -tjenester og -processer til forbundet udstyr ved at sikre privatlivets fred og cybersikkerheden og fremme øget global konkurrenceevne for Unionens IoT-industri gennem de højeste standarder for robusthed og sikkerhed;
17. FREMHÆVER i denne forbindelse behovet for at støtte SMV'er som en væsentlig byggesten i det europæiske cybersikkerhedssystem og OPFORDRER SMV'erne TIL at deltage i alle iværksatte offentlige høringer og standardiseringsaktiviteter, så der kan tages hensyn til deres værdifulde og vigtige bidrag til at gøre cybersikkerhed til et opnåeligt mål og en konkurrencefordel på det europæiske marked;
18. BEMÆRKER, at forpligtelsen til at sikre cybersikkerhed og privatlivets fred i hele et produkts livscyklus og hele dets forsyningskæde kan have en positiv indvirkning på teknologisektorens miljøaftryk ved at lede producenterne i retning af intelligente og bæredygtige udviklings- og produktionsprocesser og derved reducere mængden af elektronisk affald i forbindelse med bortskaffelse af forbundet udstyr.
