



Europeiska
unionens råd

Bryssel 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

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	2 december 2020
till:	Delegationerna

Ärende:	Rådets slutsatser om cybersäkerheten för uppkopplade enheter – Rådets slutsatser godkända genom skriftligt förfarande
---------	--

För delegationerna bifogas rådets slutsatser om cybersäkerhet för uppkopplade enheter, som godkändes av rådet genom skriftligt förfarande den 2 december 2020.

Rådets slutsatser om cybersäkerheten för uppkopplade enheter

Europeiska unionens råd

SOM ERINRAR OM

- rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU,
 - rådets slutsatser om uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU,
 - rådets slutsatser om 5G:s betydelse för den europeiska ekonomin och behovet av att minska säkerhetsriskerna i samband med 5G,
 - rådets slutsatser om framtiden för ett starkt digitaliserat Europa efter 2020: främjande av digital och ekonomisk konkurrenskraft i unionen och digital sammanhållning,
 - rådets slutsatser om att forma Europas digitala framtid,
 - Europeiska rådets slutsatser om covid-19, den inre marknaden, industripolitik, digitala frågor och yttre förbindelser,
 - meddelandet från kommissionen om att forma Europas digitala framtid,
1. FRAMHÅLLER att Europeiska unionens och dess medlemsstater måste säkerställa sin digitala suveränitet och sitt strategiska oberoende, och samtidigt bevara en öppen ekonomi; detta inbegriper att stärka förmågan att göra självständiga tekniska val och som en av de främsta pelarna, motståndskraftiga och säkra infrastrukturer, produkter och tjänster för att bygga tillit för den digitala inre marknaden och inom det europeiska samhället; Europeiska unionens grundläggande värden bevarar i synnerhet privatlivet, säkerhet, jämlikhet, mänsklig värdighet, rättsstatsprincipen och ett öppet internet som förutsättningar för att uppnå ett samhälle, en ekonomi och en industri som är digitalt drivna och människocentrerade,

2. ERKÄNNER den ökande betydelsen av uppkopplade enheter och deras säkerhet, inbegripet de maskiner, sensorer och nätverk som utgör sakernas internet; uppkopplade enheter kommer att spela en nyckelroll för att närmare forma Europas digitala framtid ur industri- och affärssynpunkt liksom i konsumenternas vardag med den nya generationens teknik; utöver 5G kan artificiell intelligens, kvantdatorteknik, högpresterande datorsystem, molntjänster, teknik för distribuerade liggare, dvs. blockkedjeteknik, och övriga nya applikationer och möjligheter till hållbar ekonomisk tillväxt och en högre nivå av digitalisering av vårt samhälle endast uppnås genom cybersäkra uppkopplade enheter,
3. NOTERAR att den ökade användningen av konsumentprodukter och industriella enheter som är uppkopplade till internet också medför nya risker för privatlivet och informations- och cybersäkerhet, inbegripet en ökande inverkan på produkters och uppgifters integritet och tillgänglighet, vilket direkt kan påverka säkerheten; det är mycket viktigt att minimera dessa risker för att skydda konsumenterna, stärka Europas övergripande cyberresiliens och förbättra medborgarnas förtroende för digitala lösningar och digital teknik; detta kommer också att främja konkurrenskraft och innovationsförmåga hos europeiska tillverkare av sådana enheter; cybersäkerhet och privatliv bör erkännas som väsentliga krav för innovation vad gäller produkter och tillverknings- och utvecklingsprocesser, även i konstruktionsfasen (inbyggd säkerhet) och bör säkerställas genom produktens hela livscykel och hela leveranskedjan,
4. BETONAR att utöver säkerställande av en hög säkerhetsnivå för uppkopplade enheter är det lika viktigt att öka konsumenternas medvetenhet om deras potentiella integritets- och säkerhetsrisker; detta skulle göra det lättare att minimera hot som härrör från ökad användning av uppkopplade enheter, öka förtroendet för den digitala inre marknaden och dra största möjliga nytta av de ekonomiska och samhällseliga fördelar som erbjuds genom uppkopplade enheters tekniska lösningar,

5. UNDERSTRYKER att behovet av offentliga investeringar i forskning och innovation, främst genom Horisont Europa och Digitala Europa, liksom privata investeringar kan skapa värdefulla incitament för att göra uppkopplade enheter säkrare och tryggare, och därmed göra smarta kommunikationsnät motståndskraftigare; investeringar i nödvändig digital infrastruktur och teknik för att införa den senaste tekniken för uppkopplade enheter bör också påskyndas för att uppnå industriellt och digitalt ledarskap, och säkerställa strategiskt oberoende, och samtidigt bevara en öppen ekonomi,
6. UNDERSTRYKER behovet av att säkerställa en hög nivå av komplementaritet och jämförbarhet för säkerhetsfunktioner i ikt-system och ikt-komponenter som används i många olika sektorer på den digitala inre marknaden,
7. KONSTATERAR den aktuella utvecklingen på unionsnivå för att höja cybersäkerhetsnivån för uppkopplade enheter, särskilt med tanke på kommissionens senaste initiativ för att på kort sikt hantera cybersäkerhetsaspekter i relevanta rättsakter, till exempel rättsakter inom den nya lagstiftningsramen inbegripet direktiv 2014/53/EU (direktivet om radioutrustning), UNDERSTRYKER vikten av att bedöma behovet av en övergripande lagstiftning, även specificering av de nödvändiga villkoren för utsläppande på marknaden, på lång sikt för att hantera alla relevanta aspekter av cybersäkerheten för uppkopplade enheter, till exempel tillgänglighet, integritet och konfidentialitet, VÄLKOMNAR i detta avseende en diskussion för att undersöka tillämpningsområdet för sådan lagstiftning och dess kopplingar till ramverket för cybersäkerhetscertifiering enligt cybersäkerhetsakten i syfte att höja säkerhetsnivån på den digitala inre marknaden,
8. UNDERSTRYKER att cybersäkerhetskrav bör fastställas i enlighet med relevant unionslagstiftning, inbegripet cybersäkerhetsakten, den nya lagstiftningsramen, förordningen om europeisk standardisering och en eventuell framtida övergripande lagstiftning, för att undvika tvetydighet och fragmentering i lagstiftningen,

9. ERKÄNNER alla berörda parter viktiga roll, särskilt tillverkarnas, för att höja cybersäkerhetsnivån för uppkopplade enheter på den digitala inre marknaden, UPPMANAR därför till samordning och nära samarbete med alla relevanta offentliga och privata berörda parter, även med avseende på en eventuell framtida övergripande lagstiftning,
- 9a. VÄLKOMNAR det pågående arbete som leds av Enisa för att upprätta en första version av EU:s ordningar för cybersäkerhetscertifiering, nämligen de föreslagna gemensamma kriterierna för Europeiska unionen och förslaget till ordning för molntjänster; dessa ordningar kommer att utgöra en viktig grund för certifieringen av uppkopplade enheter,
10. BETONAR att det i varje ytterligare certifieringsordning för uppkopplade enheter och anknutna tjänster som skulle fastställas i unionens löpande arbetsprogram och fastställas enligt cybersäkerhetsakten bör anges hur de tillämpliga säkerhetskraven på relevant tillitsnivå bör uppfyllas på grundval av specifika europeiska och internationellt erkända standarder, oavsett i vilken sektor som produkten ska användas och vilka testspecifikationer, certifikat osv. som ska tillämpas,
11. KONSTATERAR att certifieringen av uppkopplade enheter skulle kräva relevanta normer, standarder och tekniska specifikationer för utvärderingar av cybersäkerhet enligt cybersäkerhetsakten, UNDERSTRYKER därför behovet av att fastställa normer, standarder eller tekniska specifikationer vad gäller cybersäkerhet för uppkopplade enheter och REKOMMENDERAR att europeiska standardiseringsorganisationer vidtar förstärkta insatser i denna fråga, KONSTATERAR samtidigt att cybersäkerhetsstandarden (Etsi) EN 303 645 för konsumentkategorin sakernas internet är ett viktigt steg i denna riktning,

12. UPPMANAR kommissionen att behandla begäran om förslag till [...] ordningar för cybersäkerhetscertifiering av uppkopplade enheter och relaterade tjänster på grundval av unionens löpande arbetsprogram och att därvid i så stor utsträckning som möjligt beakta de övergripande europeiska ordningar för cybersäkerhetscertifiering som utarbetas för närvarande; på frivillig basis kommer en sådan ordning att möjliggöra för tillverkare av sådana produkter att marknadsföra dessa med den bedömda tillitsnivån,
13. UPPMANAR till diskussion om hur målet om cybersäkerhet kan förankras i en framtida övergripande lagstiftning som omfattar cybersäkerhetsrisker som rör uppkopplade enheter, och NOTERAR samtidigt behovet av att i förekommande fall beakta anpassningen av väsentliga krav i respektive direktiv om den nya lagstiftningsramen med avseende på reglering av marknadstillträde,
14. UPPMANAR kommissionen att vid behov också bedöma kompletterande sektorsspecifika förordningar som bör ange vilken cybersäkerhetsnivå som ska uppnås av den uppkopplade enheten för att säkerställa att specifika säkerhets- och integritetskrav införs för sådana enheter med högre säkerhetsrisker.
15. BETONAR behovet av att förbättra de europeiska medborgarnas livskvalitet och välbefinnande och uppmuntra tilltron till den digitala inre marknaden; säkerheten och integriteten i våra samhällen är avgörande för att bevara vår unions grundläggande värden, UNDERSTRYKER behovet att bygga vidare på den ram som tillhandahålls genom cybersäkerhetsakten för att harmonisera säkerhetskraven, i enlighet med olika tillitsnivåer, i alla sektorer av den nya lagstiftningsramen för att undvika fragmentering och flera kontroller av identiska krav, och erbjuder lika villkor i hela Europeiska unionen för konkurrens och innovation,

16. UPPMANAR kommissionen, EU:s byrå för cybersäkerhet (Enisa), kommittén för bedömning av överensstämmelse och marknadsövervakning inom teleområdet och europeiska gruppen för cybersäkerhetscertifiering att aktivt delta i detta initiativ för att stärka den digitala inre marknaden och stärka förtroendet för ikt-produkter, -tjänster och -processer för uppkopplade enheter genom att säkerställa integritet och cybersäkerhet och underlätta ökad global konkurrenskraft för unionens företag inom sakernas internet genom att säkerställa högsta möjliga standarder för motståndskraft, trygghet och säkerhet,
17. FRAMHÅLLER i detta sammanhang behovet av att stödja små och medelstora företag som en viktig byggsten i det europeiska ekosystemet för cybersäkerhet, och UPPMUNTRAR små och medelstora företag att delta i alla offentliga samråd som inletts liksom i standardiseringsarbetet för att beakta deras värdefulla och viktiga bidrag för att göra cybersäkerhet till ett mål som kan uppnås, och en konkurrensfördel på den europeiska marknaden,
18. NOTERAR att skyldigheten att säkerställa cybersäkerhet och integritet under en produkts hela livscykel och genom hela dess leveranskedja skulle kunna ha en positiv inverkan på tekniksektorns miljöavtryck genom att leda tillverkarna mot smarta och hållbara utvecklings- och tillverkningsprocesser och därigenom minska mängden av elektroniskt avfall som härrör från bortskaffande av uppkopplade enheter.
