Europeiska unionens råd

Bryssel den 14 september 2017
(OR. en)

12183/17
ADD 2

Interinstitutionellt ärende:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2017) 501 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN Följedokument till Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

För delegationerna bifogas dokument – SWD(2017) 501 final.

Bilaga: SWD(2017) 501 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 13.9.2017
SWD(2017) 501 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

Följedokument till

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. BEHOV AV ÅTGÄRDER

Vad är problemet och varför är det ett problem?

Den digitala tekniken och internet utgör ryggraden i EU:s ekonomi och samhälle. Viktiga ekonomiska sektorer såsom ekonomi, transport, energi, hälso- och sjukvård har blivit alltmer beroende av nät- och informationssystem för driften av kärnverksamheten. Sakernas internet kopplar samman föremål och människor via kommunikationsnät. Detta är en ny verklighet som skapar unika möjligheter men även ökar sårbarheten. Antalet cyberincidenter ökar explosionsartat, och de kommer att öka ännu mer i framtiden, både i komplexitet och frekvens och när det gäller ”utbredningen” hos konsekvenserna – alltifrån samhällsviktiga tjänster till de demokratiska processerna.

I detta sammanhang har följande sammankopplade problem konstaterats:

- En fragmentering av politiken och strategierna på cybersäkerhetsområdet i alla medlemsstater.
- Spridda resurser och insatser från EU:s institutioner, organ och byråer på cybersäkerhetsområdet.
- Bristande medvetenhet hos medborgarna och företagen om cyberhot och otillräcklig information om säkerhetsegenskaperna hos de IKT-produkter och IKT-tjänster som de köper, kombinerat med ett växande antal olika nationella och sektorsinriktade certifieringssystem.

Dessa problem påverkar EU:s övergripande cyberresiliens och leder till att den inre marknaden fungerar mindre effektivt.

Vad vill man uppnå?

Initiativet har följande specifika politiska mål:

1. Öka medlemsstaternas och företagens kapacitet och beredskap, särskilt när det gäller kritisk infrastruktur.
2. Förbättra samarbetet och samordningen mellan medlemsstaterna och EU:s institutioner, byråer och organ.
3. Öka EU:s förmåga att komplettera medlemsstaternas åtgärder, i synnerhet när det gäller gränsöverskridande cyberkriser.
4. Öka medborgarnas och företagens medvetenhet om cybersäkerhetsfrågor.
5. Öka den övergripande transparensen i fråga om assuransnivån för cybersäkerhet hos IKT-produkter och IKT-tjänster i syfte att stärka förtroendet för den digitala inre marknaden och för digital innovation.
6. Undvika en fragmentering av certifieringssystemen i EU och av de tillhörande säkerhetskraven och utvärderingskriterierna i de olika medlemsstaterna och sektorerna.

Vad är mervärdet med åtgärder på EU-nivå?

Eftersom digitaliseringen och sammanlänkningen av ekonomin och samhället har global omfattning, sträcker sig problemen långt utöver varje enskild medlemsstats territorium. Det krävs därför insatser på EU-nivå. Att döma av den nuvarande situationen och de olika framtidsscenarierna går det inte att öka unionens kollektiva cyberresiliens genom enskilda insatser från medlemsstaterna och en fragmenterad strategi för cybersäkerhet, i synnerhet med tanke på cybersäkerhetens starkt gränsöverskridande inslag.

B. LÖSNINGAR

Vilka alternativ finns för att nå målen? Finns det ett rekommenderat alternativ?

I konsekvensbedömningen undersöks en specifik uppsättning alternativ, bland annat en översyn av Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och IKT-säkerhetscertifieringen.

Översyn av Enisa

Alternativ 0 – Grundalternativ - Det här alternativet går ut på att bevara status quo. Enisas mandat skulle utvidgas, och målen och uppgifterna skulle i stort förbli oförändrade, samtidigt som de nya uppgifter Enisa fått genom senare EU-lagstiftning (t.ex. it-säkerhetsdirektivet) skulle beaktas.

Alternativ 1 – Enisas mandat löper ut (avslutande av Enisa). Det här alternativet skulle leda till att Enisa avslutas när mandatet löper ut (i juni 2020) och eventuellt till en omfördelning av befogenheterna/verksamheten på EU-nivå och/eller nationell nivå.

Alternativ 2 – En reform av Enisa. Med det här alternativet skulle bygga vidare på Enisas nuvarande mandat genom att göra selektiva förändringar som skulle beakta utvecklingen på cybersäkerhetsområdet. Byrån skulle ges ett permanent mandat som baserades på följande huvudkomponenter: stöd till utveckling och genomförande av EU:s politik, kapacitetsuppbyggnad, kunskap och information, marknadsrelaterade uppgifter, forskning och innovation, samt operativt samarbete och krishantering.

Alternativ 3 – En EU-cybersäkerhetsbyrå med full operativ kapacitet. Det här alternativet innebär att Enisa reformeras genom att tre huvudfunktioner förs samman: 1) en politisk/rådgivande uppgift, 2) ett informations- och expertcentrum, och 3) en incidenthanteringsorganisation (CERT). Det här alternativet skulle huvudsakligen innebära samma ändring av mandatets räckvidd som alternativ 2, men det skulle tillkomma uppgifter på områdena incidenthantering och krishantering, så att byråns verksamhet skulle omfatta cybersäkerhetens hela livscykel och handla om förebyggande, upptäckt och hantering av incidenter.

Certifiering

Alternativ 0 – Grundscenario – Inga åtgärder. Enligt det här alternativet skulle kommissionen bibehålla status quo och inte vidta några politiska åtgärder eller lagstiftningsåtgärder.

Alternativ 1 – Andra åtgärder än lagstiftning (”icke-bindande instrument”). Enligt det här alternativet skulle kommissionen använda icke-bindande instrument (t.ex. tolkningsmeddelanden, stöd till EU-omfattande självregleringsinitiativ och standardiseringsverksamhet) för att öka transparensen och minska fragmentiseringen.

Alternativ 2 – EU-rättsakt så att SOG-IS-avtalet omfattar alla medlemsstater. Enligt det här alternativet skulle kommissionen lägga fram ett förslag till lagstiftningsakt om att utvidga avtalet till att omfatta alla medlemsstater.

Alternativ 3 – Allmän EU-ram för IKT-cybersäkerhetscertifiering. Enligt det här alternativet skapas det ett europeiskt system för IKT-säkerhetscertifiering (som rymmer bl.a. en expertgrupp bestående av de nationella myndigheterna) på grundval av de befintliga systemen för IKT-säkerhetscertifiering. Det innebär att det blir möjligt att inrätta EU-certifieringssystem som godtas av alla medlemsstater.

Det alternativ som rekommenderas är en kombination av alternativ 2 för Enisa och alternativ 3 för certifiering.

Vilka är de olika aktörerna? Vem stöder vilket alternativ?

En stor majoritet av de intressenter från alla kategorier (medlemsstaterna, näringslivet, EU-institutionerna, forskningssamfundet) som deltog i samråden verkar välkomna det rekommenderade alternativet, eftersom de är positiva till en förstärkning av Enisa och inrättandet av en europeisk ram för IKT-säkerhetscertifiering.

I synnerhet råder det enighet om behovet av att (åtminstone) ha en väl fungerande EU-byrå med ett permanent mandat, som förses med tillräckliga resurser och lämpligt mandat för att ta itu med nuvarande och framtida utmaningar på cybersäkerhetsområdet. Det råder också bred enighet bland intressenterna om att det bör skapas en frivillig, anpassningsbar europeisk ram.

På näringslivssidan stöds den här lösningen för certifiering av de företag som redan omfattas av certifieringskrav och som skulle gynnas av en EU-omfattande mekanism baserad på ömsesidigt erkännande av certifikat. Den stöds även av de små och medelstora företagen, som skulle drabbas hårdast om de blev tvungna att genomgå flera olika certifieringsförfaranden i olika medlemsstater, eller som redan i dag tvingas göra det. Vissa medlemsstater, i synnerhet de som har mindre resurser, och vissa företrädare för industrin och EU-institutionerna var även positiva till alternativ 3 för Enisa.

C. DET REKOMMENDERADE ALTERNATIVETS KONSEKVENSER

Vilka fördelar har det rekommenderade alternativet (om ett sådant alternativ finns, i annat fall huvudalternativen)?

Enligt det rekommenderade alternativet skulle EU inrätta en byrå som är inriktad på att ge stöd till medlemsstaterna, EU-institutionerna och företagen på de områden där den skulle ha störst mervärde. Dessa områden omfattar stöd till genomförandet av it-säkerhetsdirektivet, utveckling och genomförande av politiken, information, kunskap och medvetandehöjande, forskning, operativt samarbete och krishantering, och marknaden. Enisa skulle särskilt stödja EU:s politik på området IKT-säkerhetscertifiering genom att svara för det administrativa underhållet och den tekniska förvaltningen av en europeisk ram för IKT-säkerhetscertifiering.

Genom en sådan ram kan man på ett verksamt sätt införa en uppsättning regler som styr IKT-säkerhetscertifieringen i EU, vilket skulle främja ett system med ömsesidigt erkännande av de certifikat som utfärdas i de olika medlemsstaterna. Lösningen att kombinera de här alternativen har bedömts vara den mest effektiva för att EU ska nå de fastställda målen att öka kapaciteten, beredskapen, samarbetet, medvetenheten och transparensen på cybersäkerhetsområdet, och undvika en fragmentering av marknaden. Den här lösningen är också den som bäst överensstämmer med de politiska prioriteringarna, eftersom den är förankrat i strategin för cybersäkerhet och tillhörande politik (t.ex. it-säkerhetsdirektivet) och med strategin för den digitala inre marknaden. Dessutom skulle målen nås med rimligt utnyttjande av resurser om det här alternativet valdes.

Vad är kostnaderna för det rekommenderade alternativet (om ett sådant alternativ finns, i annat fall huvudalternativen)?

Även om Enisa skulle ges nya roller, skulle byrån förbli en smidig organisation även efter reformen. Det ekonomiska bidraget från EU-budgeten skulle bli högre än i dag men fortfarande lågt jämfört med andra organ som också är verksamma inom kritiska områden.

Inrättandet av en europeisk ram för IKT-säkerhetscertifiering skulle inte medföra ytterligare initialkostnader för företagen (inklusive de små och medelstora företagen). Det skulle tvärtom skapa betydande besparingar för de företag som redan certifierar sina produkter eller är villiga att göra det, något som skulle gynna deras konkurrenskraft internationellt. Å andra sidan skulle det krävas vissa budgetåtaganden för underhållet av ramen, vilket Enisa i dess reformerade utförande huvudsakligen skulle åta sig när det gäller de tekniska uppgifterna och sekretariatsuppgifterna.

Påverkas medlemsstaternas budgetar och förvaltningar i betydande grad?

Nej. Kostnaderna i samband med förstärkningen av Enisa skulle främst belasta EU-budgeten, medan medlemsstaterna skulle kunna lämna frivilliga ekonomiska bidrag till byrån. När det gäller certifiering skulle den huvudsakliga påverkan på de nationella budgetarna och förvaltningarna komma från inrättandet av en certifieringsmyndighet när så är nödvändigt.

Uppstår andra betydande konsekvenser?

Nej.

Proportionalitetsprincipen

Det rekommenderade alternativet omfattar väl avvägda åtgärder som samtliga anses nödvändiga för att målet ska kunna uppnås utan att det medför några orimliga bördor för berörda aktörer. Mot bakgrund av detta bedöms det här initiativet vara förenligt med proportionalitetsprincipen.

D. UPPFÖLJNING

När kommer åtgärderna att ses över?

Enligt det nuvarande förslaget ska den första utvärderingen ske fem år efter det rättsliga instrumentets ikraftträdande. Kommissionen kommer sedan att avlägga rapport till Europaparlamentet och rådet om sin utvärdering, vid behov åtföljd av ett förslag om översyn av direktivet. Därefter ska utvärderingar göras vart femte år.