EUROPA-
KOMMISSIONEN

Bruxelles, den 13.9.2017
COM(2017) 478 final

RAPPORT FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om evalueringen af Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA)

1. INDLEDNING

1.1 ENISA

Den Europæiske Unions Agentur for Net- og Informationssikkerhed ("ENISA") blev oprettet i 2004 og har fået sit mandat fornyet med jævne mellemrum. ENISA's aktuelle mandat er fastsat i forordning EU nr. 526/2013[1] (i det følgende benævnt "ENISA-forordningen") og udløber den 19. juni 2020.

ENISA's mandat er at bidrage til et højt net- og informationssikkerhedsniveau i Unionen. ENISA-forordningen beskriver de specifikke mål for Agenturet og fastsætter, at det skal:

- udvikle og fastholde et højt ekspertiseniveau
- bistå Unionens institutioner, organer, kontorer og agenturer med at udarbejde de nødvendige politikker for net- og informationssikkerhed
- bistå Unionens institutioner, organer, kontorer og agenturer og medlemsstaterne med at gennemføre de politikker, der er nødvendige for at opfylde de retlige og reguleringsmæssige krav vedrørende net- og informationssikkerhed i henhold til eksisterende og fremtidige EU-retsakter og dermed bidrage til et velfungerende indre marked
- bistå Unionen og medlemsstaterne med at øge og styrke deres kapacitet og beredskab til at forebygge, opdage og imødegå net- og informationssikkerhedsproblemer og -hændelser
- bruge sin ekspertise til at fremme et bredt samarbejde mellem aktører fra både den offentlige og den private sektor.

Herudover besluttede EU-medlovgiverne med direktiv (EU) 2016/1148[2] om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet), at tildele ENISA vigtige roller i forbindelse med gennemførelsen af lovgivningen. Agenturet varetager navnlig sekretariatsfunktionen for CSIRT-netværket (oprettet for at fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne), og det bistår også samarbejdsgruppen for strategisk samarbejde med udførelsen af dens opgaver. Herudover pålægger direktivet ENISA at bistå medlemsstaterne og Kommissionen med ekspertise og rådgivning og at lette udveksling af bedste praksis.

Agenturet har sit hjemsted i Grækenland med det administrative sæde i Heraklion (Kreta) og det centrale operationelle hovedsæde i Athen. Det har 84 ansatte og et årligt driftsbudget på 11,25 mio. EUR. Det ledes af en administrerende direktør, og forvaltningen varetages af en bestyrelse, et forretningsudvalg og en stående gruppe af interessenter. Et uformelt netværk af nationale forbindelsesofficerer faciliterer kontakten med medlemsstaterne.

1.2 RAPPORTENS FORMÅL

Ifølge artikel 32 i ENISA-forordningen skal Kommissionen få foretaget en evaluering af ENISA inden den 20. juni 2018 for "navnlig at vurdere virkningen, effektiviteten og

[1] http://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1495472820549&uri=CELEX:32013R0526
[2] http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

produktiviteten af agenturets arbejde og dets arbejdsmetoder" og for at tage stilling til, om det aktuelle mandat bør forlænges.

I lyset af de betydelige ændringer, der er sket inden for cybersikkerhed siden 2013, hvor den nuværende ENISA-forordning blev vedtaget – og med tanke på det nåede modenhedsniveau på det politiske, markedsmæssige og teknologiske plan – bekendtgjorde Kommissionen i sin meddelelse fra 2016 om styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri[3], at den ville fremskynde evalueringen og revisionen af ENISA. Kommissionen bemærkede især, at revisionen af ENISA ville være en anledning til at se nærmere på den mulige forbedring af Agenturets kapaciteter og muligheder for på bæredygtig vis at støtte medlemsstaterne i deres bestræbelser på at opnå modstandsdygtighed over for cyberangreb.

Denne vision blev yderligere styrket af Rådets konklusioner i 2016[4], som anerkendte, "at cybertrusler og sårbarheder fortsat udvikler sig og tiltager, hvilket vil kræve vedvarende og tættere samarbejde, særlig ved håndteringen af væsentlige grænseoverskridende cybersikkerhedshændelser". Konklusionerne bekræftede, at "ENISA-forordningen er et af de centrale elementer i EU's ramme for modstandsdygtighed over for cyberangreb".

Resultaterne af ENISA-evalueringen er blevet brugt i den konsekvensanalyse, der ledsager forslaget til en forordning om Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA, "EU's Agentur for Cybersikkerhed") og om ophævelse af forordning (EU) nr. 526/2013 og om sikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed").

I henhold til artikel 32 i ENISA-forordningen sender Kommissionen evalueringsrapporten og dens konklusioner til Europa-Parlamentet, Rådet og bestyrelsen. Denne sammenfattende rapport ledsages af et arbejdsdokument fra Kommissionens tjenestegrene om evalueringen af Den Europæiske Unions Agentur for Net- og Informationssikkerhed (SWD(2017) 502).

2. DE VIGTIGSTE RESULTATER AF EVALUERINGEN

I overensstemmelse med Kommissionens retningslinjer for bedre regulering[5] har Kommissionen vurderet Agenturets effektivitet, omkostningseffektivitet, sammenhæng, relevans og EU-merværdi med hensyn til dets resultater, styring, intern organisatorisk struktur og arbejdsmetoder.

Analysen tog også højde for den ændrede kontekst, som Agenturet fungerer i nu, med hensyn til de nye lovgivningsmæssige og politiske EU-rammer (f.eks. NIS-direktivet, revisionen af EU's strategi for cybersikkerhed), de ændrede behov hos Agenturets interessenter og komplementaritet og mulige synergier med det arbejde, der udføres af andre af EU's og medlemsstaternes institutioner, agenturer og organer såsom IT-beredskabet for EU's institutioner, agenturer og organer (CERT-EU) og Det Europæiske center til Bekæmpelse af IT-Kriminalitet (EC3) hos Europol.

---

[3] Kommissionens meddelelse om styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri, COM/2016/0410 final.

[4] Rådets konklusioner om styrkelse af Europas modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri – 15. november 2016.

[5] COM (2015)215final SWD (2015)111 final; http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf

Med henblik på at evaluere Agenturets funktion:

- Har Kommissionen fået udarbejdet en uafhængig undersøgelse, som blev gennemført fra november 2016 til juli 2017, og som udgør den vigtigste kilde til evalueringen sammen med de interne analyser, som Kommissionen har gennemført.
- Undersøgelsen omfattede dokumentationsundersøgelser, dataindsamling og -analyse, herunder interessentrundspørger, dybdegående interviews med centrale aktører inden for cybersikkerhedsområdet, en interessentworkshop, benchmarking, en positioneringsundersøgelse for Agenturet og en analyse af styrker, svagheder, muligheder og trusler (SWOT-analyse).
- Har Kommissionen gennemført en offentlig onlinehøring på 12 uger, som dækkede både det tidligere og fremtidige ENISA, og målrettede høringer med de vigtigste interessenter.

Evalueringens vigtigste resultater, i henhold til evalueringskriterierne, kan sammenfattes som følger:

1. **Relevans:** I en kontekst med hurtig teknologisk udvikling og skiftende trusler og i betragtning af det betydelige behov for øget net- og informationssikkerhed (NIS) i EU har ENISA's mål vist sig at være relevante. Det forholder sig faktisk sådan, at medlemsstater og EU-organer har brug for ekspertise om NIS, og der må opbygges kapacitet i medlemsstaterne til at forstå og imødegå trusler, og interessenterne må samarbejde på tværs af temaområder og institutioner. NIS er fortsat en central politisk prioritet for EU, hvor ENISA forventes at reagere, men ENISA's udformning som et EU-agentur med en tidsbegrænset mandatperiode giver i) ikke mulighed for langsigtet planlægning og bæredygtig støtte til medlemsstaterne og EU-institutionerne i den hurtigt vekslende cybersikkerhedssituation og kan ii) føre til et juridisk tomrum, idet bestemmelserne i NIS-direktivet, som overdrager opgaver til ENISA, har en permanent karakter.

2. **Effektivitet:** ENISA har samlet set nået sine mål og løst sine opgaver. Det bidrog til at øge NIS i Europa via sine vigtigste aktiviteter (kapacitetsopbygning, tilrådighedsstillelse af ekspertise, fællesskabsopbygning og støtte til politikker). Der var dog potentiale for forbedringer i forhold til alle aktiviteter. Evalueringen konkluderede, at ENISA effektivt har skabt stærke og tillidsfulde forhold til nogle af interessenterne, herunder navnlig medlemsstaterne og CSIRT'erne. Indgreb inden for kapacitetsopbygning blev opfattet som effektive, navnlig i medlemsstater med få ressourcer. Stimulering af bredt samarbejde har været et af højdepunkterne, og interessenterne er enige om den positive rolle, som ENISA spiller for at bringe aktørerne sammen. ENISA havde dog svært ved at have en stor virkning på det store NIS-område. Det skyldtes også, at der var forholdsvis begrænsede menneskelige og finansielle ressourcer til at dække et meget bredt mandat. Evalueringen konkluderede også, at ENISA delvist opfyldte målet om at yde ekspertise, hvilket hang sammen med problemer med at rekruttere eksperter (se også afsnittet om omkostningseffektivitet).

3. **Omkostningseffektivitet:** Til trods for sit lille budget – blandt de laveste sammenlignet med andre EU-agenturer – formåede Agenturet at bidrage til specifikke målsætninger, og udnyttede generelt sine ressourcer på en omkostningseffektiv måde. Evalueringen konkluderede, at processerne generelt

var effektive, og der var en klar afgrænsning af ansvar i organisationen, som førte til en god gennemførelse af arbejdet. En af de største udfordringer for Agenturets omkostningseffektivitet vedrører ENISA's vanskeligheder med at rekruttere og fastholde højt kvalificerede eksperter. Resultaterne viser, at dette kan forklares med en kombination af faktorer, herunder de generelle vanskeligheder i hele den offentlige sektor med at konkurrere med den private sektor, når det forsøges at ansætte højt specialiserede eksperter, den type kontrakter (tidsbegrænset), som Agenturet oftest kunne tilbyde, og ENISA's placering, som ikke anses for så attraktiv, f.eks. i forbindelse med ægtefællers mulighed for at finde arbejde. En placering fordelt mellem Athen og Heraklion medførte en ekstra koordineringsindsats og ekstra omkostninger, men flytningen til Athen i 2013 af den centrale operationelle afdeling øgede Agenturets operationelle omkostningseffektivitet.

4. **Sammenhæng:** ENISA's aktiviteter har generelt været i overensstemmelse med interessenternes politikker og aktiviteter på nationalt plan og på EU-plan, men der er behov for en mere koordineret tilgang til cybersikkerhed på EU-plan. Potentialet for samarbejde mellem ENISA og andre EU-organer er ikke blevet udnyttet fuldt ud. Udviklingen i EU's juridiske og politiske landskab gør, at det aktuelle mandat nu er mindre sammenhængende.

5. **Merværdi for EU:** ENISA's merværdi ligger primært i Agenturets evne til at forbedre samarbejdet, hovedsageligt mellem medlemsstaterne, men også med beslægtede NIS-fælleskaber. Der findes ingen anden aktør på EU-plan, der støtter samarbejdet mellem det samme udsnit af interessenter inden for NIS-området. Agenturets merværdi var forskelligt, alt efter dets interessenters forskellige behov og ressourcer (f.eks. store i forhold til små medlemsstater, medlemsstater i forhold til erhvervslivet) og Agenturets behov for at prioritere sine aktiviteter i overensstemmelse med arbejdsprogrammet. Evalueringen konkluderede, at en mulig lukning af ENISA ville være en tabt mulighed for alle medlemsstater. Det ville ikke være muligt at sikre samme grad af fælleskabsopbygning og samarbejde på tværs af medlemsstaterne inden for cybersikkerhed uden et decentralt EU-agentur. Der ville ske en større opsplitning, hvor bilateralt eller regionalt samarbejde ville opstå for at fylde tomrummet efter ENISA.

3. KONKLUSIONER/ANBEFALINGER

Evalueringen konkluderede, at ENISA havde fået overdraget et bredt mandat ved ENISA-forordningen – hvilket giver fleksibilitet, men i nogle tilfælde mangler fokus, som gør det vanskeligt for Agenturet at opnå en stor virkning – og at Agenturets mål har vist sig at være relevante i perioden 2013-2016. Agenturet opnåede en høj grad af effektivitet og påviste merværdien af at handle på EU-plan, navnlig gennem centrale aktiviteter såsom de fælleseuropæiske Cyber Europe-øvelser, støtten til CSIRT-netværket og analyser af trusselsbilledet. ENISA har bidraget til at øge net- og informationssikkerheden i EU, hovedsageligt ved at støtte samarbejdet mellem medlemsstaterne og net- og informationssikkerhedsinteressenter, samt gennem sine fællesskabs- og kapacitetsopbygningsaktiviteter.

Agenturet opnåede disse resultater trods en række udfordringer, som blev præsenteret i den foregående del af denne rapport og det vedlagte arbejdsdokument fra Kommissionens tjenestegrene. En af de vigtigste udfordringer var knyttet til de begrænsede ressourcer, som ikke svarede til Agenturets brede mandat, navnlig i betragtning af de nye opgaver, som tillægges Agenturet ved NIS-direktivet, og det hurtigt

skiftende trusselsbillede. ENISA er også fortsat det eneste EU-agentur med et tidsbegrænset mandat til trods for bl.a. opgaver i forbindelse med NIS-direktivet, som nævnt ovenfor.

Cybersikkerhedstrusselsbilledet udvikler sig hurtigt med nye trusler i takt med, at EU bliver stadig mere afhængig af digital infrastruktur og digitale tjenester, ikke kun via forbundet udstyr, men også den allestedsnærværende konnektivitet. Tingenes Internet skaber nye muligheder i forbindelse med energieffektivitet, miljøbeskyttelse, forbundet mobilitet, sundhedsovervågning i realtid og intelligente og gnidningsløse finansielle transaktioner i den digitale økonomi og det digitale samfund. Hånd i hånd med disse drivkræfter går dog også nye sårbarheder og angrebsværktøjer, som gør det muligt at udnytte kompromitteret udstyr til at skabe forstyrrelser i det indre digitale marked.

Evalueringen førte frem til den konklusion, at det nuværende mandat for ENISA ikke giver Agenturet de nødvendige værktøjer til at imødegå nuværende og fremtidige cybersikkerhedsudfordringer.

Derudover er der en tiltagende risiko for øget opsplitning af markedet på EU-plan på grund af en række aktører på EU-plan inden for cybersikkerhed og utilstrækkelig koordinering mellem dem. EU har brug for et centralt punkt til at håndtere nye trusler, som i deres natur er horisontale og indvirker på mange industrisektorer samt til at opfylde behovene hos cybersikkerhedsfællesskabet, herunder navnlig hos medlemsstaterne, EU-institutionerne og erhvervslivet. Evalueringen kommer frem til, at der er behov for et EU-agentur, som er organiseret på tværs af sektorer/horisontalt med et stærkt mandat.

Evalueringen viser, at til trods for en række udfordringer er der betydelige muligheder for ENISA, hvis det udstyres med et tilstrækkeligt mandat og støtte i form af finansielle og menneskelige ressourcer, til at yde et bidrag til øget cybersikkerhed i EU.

Der er også et klart behov for samarbejde og koordinering på tværs af forskellige interessenter. Behovet for en koordinerende enhed på EU-plan til at facilitere informationsstrømme, udfylde huller og undgå overlapning af roller og ansvarsområder bliver stadig mere akut. ENISA vil som et decentralt EU-agentur og en neutral mægler være i stand til at koordinere EU's tilgang til cybertrusler.

På denne baggrund har Kommissionen fremsat et forslag til en reform af ENISA, som giver Agenturet et permanent mandat, som bygger på dets vigtigste styrker og de nye prioriterede indsatsområder, f.eks. inden for cybersikkerhedscertificering. Dette nye mandat bør afspejle de ændrede realiteter og bemyndige agenturet til på passende vis at understøtte EU fremover.