EUROPEISKA
KOMMISSIONEN

Bryssel den 5.7.2016
COM(2016) 410 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

Stärka Europas system för cyberresiliens

och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch

1. INLEDNING/BAKGRUND

Varje dag inträffar cybersäkerhetsincidenter med allvarliga ekonomiska konsekvenser för de europeiska företagen och ekonomin som helhet. Sådana incidenter undergräver medborgarnas och företagens förtroende för det digitala samhället. Stöld av affärshemligheter, företagsinformation och personuppgifter, störningar av tjänster – även mycket viktiga sådana – och infrastruktur medför ekonomiska förluster som uppgår till hundratals miljarder euro varje år[1]. Detta kan också påverka medborgarnas grundläggande rättigheter och samhället i stort.

Den politiska kärnan i Europeiska unionens åtgärder mot sådana cybersäkerhetsutmaningar utgörs av Europeiska unionens strategi för cybersäkerhet från 2013 (EU-strategin för cybersäkerhet)[2], som framför allt mynnade ut i det snart antagna direktivet om nät- och informationssäkerhet[3], samt direktiv 2013/40 om angrepp mot informationssystem. EU har också specialiserade organ till sitt förfogande, bl.a. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), Europeiska it-brottscentrumet (EC3) vid Europol och organisationen för incidenthantering (Cert-EU). På senare tid har också ett antal sektorsspecifika initiativ inletts (t.ex. på energi- och transportområdet) för att öka cybersäkerheten inom olika kritiska sektorer.

Trots dessa framsteg har EU fortfarande otillräckligt skydd mot cyberincidenter, vilket kan undergräva den digitala inre marknaden, det ekonomiska livet och samhällslivet i stort. Konsekvenserna begränsar sig inte nödvändigtvis till ekonomin. Vid hybridhot[4] kan cyberattacker samordnas med andra åtgärder för att destabilisera ett land eller utmana politiska institutioner.

Mot denna bakgrund kan hanteringen av storskaliga cyberincidenter som berör flera medlemsstater samtidigt innebära en utmaning för EU. Med ett samlat grepp, som beaktar meddelandet om motverkande av hybridhot och meddelandet om att genomföra den europeiska säkerhetsagendan[5], undersöker kommissionen hur den föränderliga cybersäkerhetssituationen kan angripas och analyserar vilka ytterligare åtgärder som kan behövas för att öka EU:s cybersäkerhetsresiliens och förmåga att hantera incidenter.

Kommissionen arbetar också med industriell cybersäkerhetskapacitet i EU. Även om inte hela värdekedjan för digital teknik kan bemästras i Europa måste vi åtminstone bibehålla och utveckla viss grundläggande kapacitet. Tillhandahållandet av produkter och tjänster som garanterar högsta nivå av cybersäkerhet innebär en möjlighet för den europeiska cybersäkerhetsbranschen som skulle kunna bli en stor konkurrensfördel. Den globala marknaden för cybersäkerhet förväntas bli ett av de snabbast växande segmenten av IKT-sektorn[6]. Om EU ska kunna bli en ledande aktör på detta område måste vi fastställa stränga

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, Center for Strategic and International Studies; juni 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.
[6] Se SWD(2016) 216.

datasäkerhetsvillkor, även för personuppgifter, och måste vi reagera effektivt vid intrång. Detta kommer att ses som ett starkt argument för investeringar i EU och därigenom bidra till de ambitiösa målen för den digitala inre marknaden för att skapa tillväxt och sysselsättning.

Det behövs ett starkt åtagande för att uppnå detta, särskilt genom följande:

i) Ett intensifierat samarbete för att stärka beredskapen och hantera cyberincidenter.

Existerande och överenskomna samarbetsmekanismer måste stärkas för att öka EU:s resiliens och beredskap, även för eventuella europaomfattande cybersäkerhetskriser. Dessa samarbetsmekanismer bör omfatta hela incidenternas livscykel, från förebyggande åtgärder till åtal. För ett effektivt samarbete mellan medlemsstaterna och det praktiska genomförandet av säkerhetskraven för kritiska operatörer krävs också robusta tekniska lösningar från cybersäkerhetsbranschen.

Om man ska säkerställa resiliens hos kritiska cybertillgångar i hela EU kommer det samtidigt att krävas kontinuerliga ansträngningar för att hitta sektorsövergripande synergier och skapa enhetliga cyberkrav inom alla relevanta EU-politikområden. Kommissionen kommer inom en snar framtid att ta ställning till behovet av att uppdatera 2013 års EU-strategi för cybersäkerhet.

ii) Utmaningar på Europas inre marknad för cybersäkerhet

I strategin för den digitala inre marknaden[7] konstateras det att det fortfarande finns tydliga luckor på det snabbrörliga området teknik och lösningar för nätsäkerhet. Samtidigt visar marknadsundersökningar att EU:s inre marknad fortfarande är geografiskt fragmenterad när det gäller tillhandahållande av cybersäkerhetsprodukter och -tjänster[8]. I detta meddelande beskrivs ett antal marknadsinriktade politiska åtgärder för att åtgärda dessa utmaningar och brister på den inre marknaden.

iii) Främjande av industriell kapacitet på för området cybersäkerhet

I EU-strategin för cybersäkerhet och strategin för den digitala inre marknaden förband sig kommissionen att främja ett ökat utbud av produkter och tjänster från EU:s cybersäkerhetsindustri. Därför kommer kommissionen också att anta ett beslut som banar väg för avtal om offentlig-privata partnerskap avseende cybersäkerhet, som inriktas på att utveckla europeisk spetsforskning och en innovationsagenda på cybersäkerhetsområdet för att öka konkurrenskraften.

2. EN NY NIVÅ AV SAMARBETE, KUNSKAPER OCH KAPACITET

EU-strategin för cybersäkerhet, och i synnerhet det kommande direktivet om nät- och informationssäkerhet[9], kommer att bana väg för bättre samarbete på EU-nivå mellan medlemsstaterna. Ett snabbt och effektivt genomförande av direktivet kommer att vara

[7] COM(2015) 192.
[8] Se SWD(2016) 216.
[9] Direktivet om nät- och informationssäkerhet kommer att ålägga medlemsstaterna att identifiera ett antal operatörer av grundläggande tjänster inom sådana områden som energi, transport, finanser och hälso- och sjukvård, för att åtgärda cybersäkerhetsrisker, och att se till att vissa leverantörer av digitala tjänster vidtar ändamålsenliga åtgärder för att åtgärda sådana risker.

avgörande med tanke på den ökande digitaliseringen av ekonomin och samhällslivet (även med beaktande av molntjänster, sakernas internet och kommunikation från maskin till maskin), det ökade antalet gränsöverskridande sammanlänkningar och cyberhotens snabba utveckling[10]. EU måste förbereda sig på möjligheten av storskaliga cyberkriser[11], som t.ex. samtidiga angrepp mot kritiska informationssystem i flera medlemsstater[12].

Därför är samarbetet på EU-nivå avgörande för att man ska kunna hantera både småskaliga men potentiellt allt vanligare cyberincidenter och en eventuell storskalig cyberattack i flera medlemsstater. EU måste beakta cyberaspekter i de befintliga mekanismerna för krishantering. EU måste också säkerställa effektiva mekanismer för samarbete och snabbt informationsutbyte mellan olika sektorer och medlemsstater för att begränsa och reagera på sådana incidenter. Dessa mekanismer bör fungera på ett enhetligt sätt och därigenom bidra till kampen mot terrorism, organiserad brottslighet och cyberbrottslighet. Detta kan även stärka EU:s förmåga att samordna arbetet med sina internationella partner för att kunna bemöta globala hot och incidenter på ett effektivt sätt.

2.1. Bästa användning av samarbetsmekanismer enligt direktivet om nät- och informationssäkerhet och utveckling mot Enisa 2.0

En väsentlig del av den nationella kapacitet som krävs enligt direktivet om nät- och informationssäkerhet utgörs av arbetsgrupper för åtgärder vid datorincidenter (CSIRT) som ansvarar för snabba reaktioner på cyberhot och cyberincidenter. De kommer att bilda ett CSIRT-nätverk för att främja ett effektivt operativt samarbete om specifika cybersäkerhetsincidenter och informationsutbyte om risker. Genom direktivet kommer också en samarbetsgrupp att inrättas för att stödja och underlätta det strategiska samarbetet mellan medlemsstaterna och bygga upp förtroendet mellan dem.

Med tanke på cyberhotens art och mångfald uppmuntrar kommissionen medlemsstaterna att utnyttja direktivets samarbetsmekanismer maximalt och öka det gränsöverskridande samarbetet om beredskap inför storskaliga cyberincidenter. Sådant ytterligare samarbete vid betydande cyberincidenter skulle gagnas av en samordnad strategi för krissamarbete mellan de olika delarna av cyberekosystemet. En sådan strategi kan vara i form av en konkret plan, som även bör säkerställa synergieffekter och samstämmighet med befintliga krishanteringsmekanismer[13]. Strategin bör därefter testas regelbundet vid cybersäkerhetsövningar och andra krishanteringsövningar. EU-organ som Enisa, CERT-EU och det europeiska centrumet mot it-brottslighet (EC3) vid Europol bör också ha en roll inom strategin, som kan baseras på verktyg som utvecklats inom CSIRT-nätverket. Under första halvåret 2017 kommer kommissionen att lägga fram en sådan samarbetsplan så att samarbetsgruppen, CSIRT-nätverket och andra berörda intressenter kan ta ställning till den.

Det finns redan i dag kunskap och expertis på EU-nivå när det gäller cybersäkerhet, men den är splittrad och ostrukturerad. För att stödja samarbetsmekanismerna inom ramen för

[10] Se SWD(2016) 216.
[11] Se t.ex. Enisas rapport: *Common practices of EU-level crisis management and applicability to cyber crises* (april 2016).
[12] Se SWD(2016) 216.
[13] Särskilt EU-arrangemangen för integrerad politisk krishantering, inklusive beslutet om närmare bestämmelser för unionens genomförande av solidaritetsklausulen (24 juli 2014) och beslutsprocesserna inom den gemensamma säkerhets- och försvarspolitiken.

direktivet om nät- och informationssäkerhet bör man samla informationen i ett ”informationsnav” som gör den lättillgänglig på begäran för samtliga medlemsstater. Informationsnavet skulle vara en central resurs så att EU-institutionerna och medlemsstaterna kan utbyta information på lämpligt sätt. Enklare tillgång till bättre strukturerad information om cybersäkerhetsrisker och tänkbara åtgärder bör hjälpa medlemsstaterna att öka sin kapacitet och anpassa sin praxis, och därigenom stärka den allmänna motståndskraften mot attacker. Kommissionen kommer, med stöd av Enisa, CERT-EU och med hjälp av expertis från det gemensamma forskningscentrumet, att verka för att ett sådant informationsnav skapas och säkerställa dess långsiktiga hållbarhet.

En reguljär rådgivande högnivågrupp[14] för cybersäkerhet bör inrättas på EU-nivå och bestå av experter och beslutsfattare från näringslivet, den akademiska världen, civilsamhället och andra berörda organisationer. Gruppen kan ge kommissionen tillgång till extern expertis och synpunkter utifrån, på ett öppet och transparent sätt, som sedan kan ligga till grund för politiska strategier för cybersäkerhet, potentiella regleringsåtgärder eller andra politiska åtgärder. Gruppen skulle komplettera och samverka med andra strukturer för cybersäkerhet[15] .

Kommissionen ska senast 20 juni 2018 utvärdera Enisa, och eventuella ändringar eller förlängningar av Enisas mandat ska antas senast den 19 juni 2020[16]. Mot bakgrund av det nuvarande cybersäkerhetslandskapet avser kommissionen att snabba på utvärderingen och, beroende på resultatet, lägga fram ett förslag snarast möjligt.

När kommissionen bedömer om Enisas mandat behöver ändras kommer den att beakta de cybersäkerhetsutmaningar som beskrivs ovan och de övergripande insatserna för att intensifiera samarbetet och kunskapsutbytet. Genom denna process kommer man att kunna undersöka hur man skulle kunna stärka byråns kapacitet för att stödja medlemsstaterna på ett hållbart sätt när det gäller att uppnå cybersäkerhetsresiliens. Analysen av Enisas mandat skulle också behöva ta hänsyn till byråns nya ansvarsområden enligt direktivet om nät- och informationssäkerhet, nya mål för att stödja cybersäkerhetsbranschen (strategin för den digitala inre marknaden och i synnerhet de offentlig-privata partnerskapen), nya behov för att trygga kritiska sektorer och nya utmaningar i samband med gränsöverskridande incidenter, inklusive samordnade åtgärder mot cyberkriser.

Kommissionen kommer att göra följande:

- Lägga fram en samarbetsplan för hanteringen av storskaliga cyberincidenter på EU-nivå under första halvåret 2017.
- Främja inrättandet av ett informationsnav för att främja informationsutbyte mellan EU-organ och medlemsstaterna.
- Inrätta en rådgivande högnivågrupp för cybersäkerhet.
- Slutföra utvärderingen av Enisa före utgången av 2017. I samband med utvärderingen ska man ta ställning till om Enisas mandat behöver ändras eller

[14] Kommissionens expertgrupper omfattas av de övergripande bestämmelser som fastställs i kommissionens beslut C(2016)3301.
[15] T.ex. plattformen för nät- och informationssäkerhet, det offentligprivata partnerskapet för cybersäkerhet och sektoriella plattformar, som t.ex. EECSP (*Energy Expert Cyber Security Platform*). Den bör även kopplas till den högnivågrupp som aviserades i meddelandet om digitalisering av den europeiska industrin: COM(2016) 180.
[16] Förordning (EU) nr 526/2013 om upphävande av förordning (EG) nr 460/2004.

utvidgas, med målet att ta fram ett eventuellt förslag så snart som möjligt.

2.2 Ökade insatser för utbildning och övning på cybersäkerhetsområdet

Tillräcklig kompetens och utbildning för att både förhindra cybersäkerhetsincidenter och begränsa sådana incidenters effekter är ett par viktiga aspekter för att uppnå cybersäkerhetsresiliens.

I dag har Enisa och Ecteg (*European Cybercrime Training and Education Group*), i samarbete med det europeiska centrumet mot it-brottslighet vid Europol och Europeiska polisakademin (Cepol), en viktig funktion när det gäller att stödja kapacitetsuppbyggnad, även när det gäller cyberrelaterad kriminalteknik, genom att ta fram handböcker och anordna utbildning och cybersäkerhetsövningar.

Samtidigt är cyberrymden ett område som förändras snabbt och där kapacitet med dubbla användningsområden spelar en avgörande roll. Därför är det nödvändigt att utveckla ett civilt-militärt samarbete och synergier inom utbildning och övningar för att förbättra resiliensen och kapaciteten för incidenthantering i EU.

Mot bakgrund av detta, och som en uppföljning av antagandet av direktivet om nät- och informationssäkerhet och ramen för EU:s politik för it-försvar[17], kommer kommissionens avdelningar att samarbeta med medlemsstaterna, Europeiska utrikestjänsten (EEAS), Enisa och andra berörda EU-organ[18] för att inrätta en plattform för utbildning och övning på cybersäkerhetsområdet som kommer att främja synergier mellan civil och militär utbildning.

Kommissionen kommer att göra följande:

- Upprätta ett nära samarbete med medlemsstaterna, Enisa, Europeiska utrikestjänsten och andra berörda EU-organ för att inrätta en plattform för utbildning i cybersäkerhet.

2.3. Ömsesidiga beroendeförhållanden mellan sektorer och resiliens för den oumbärliga offentliga nätinfrastrukturen

En viktig faktor när man ska bedöma risken för och konsekvenserna av en storskalig cyberincident är graden av ömsesidigt beroende över gränser och mellan sektorer En allvarlig cyberincident inom en sektor eller medlemsstat kan direkt eller indirekt påverka – eller spridas till – andra sektorer eller andra medlemsstater.

Ett samarbete över gränser och mellan sektorer främjar utbytet av information och expertis och ökar därmed beredskapen och resiliensen. Kommissionen har stött arbete inom olika

[17] Antaget av rådet (utrikes frågor) den 18 november 2014, dok. 15585/14.
[18] T.ex. Europeiska säkerhets- och försvarsakademin, EC3, Cepol och Europeiska försvarsbyrån.

sektorer som syftar till att öka kunskapen om beroendeförhållanden genom genomförandet av det europeiska programmet för skydd av kritisk infrastruktur[19].

En nödvändig förutsättning för hanteringen av sektorsöverskridande risker kommer samtidigt att vara de enskilda sektorernas förmåga att identifiera, förbereda sig inför och reagera på cyberincidenter. Kommissionen kommer att bedöma riskerna till följd av cyberincidenter inom sektorer med stort ömsesidigt beroende inom och över nationella gränser, i synnerhet sektorer som omfattas av direktivet om nät- och informationssäkerhet. Kommissionen kommer då även att beakta den internationella utvecklingen[20]. Utifrån denna bedömning kommer kommissionen att ta ställning till om det behövs ytterligare särskilda bestämmelser och/eller vägledning om beredskapen inför cyberrisker inom sådana kritiska sektorer.

På europeisk nivå kan sektorsvisa centrum för informationsutbyte och analys (ISAC)[21] och motsvarande CSIRT-enheter ha en viktig roll i beredskapen inför och reaktionerna på cyberincidenter. För att garantera effektiva informationsflöden om nya hot och underlätta åtgärder vid cyberincidenter bör ISAC-centrumen uppmuntras att samarbeta med CSIRT-nätverken enligt direktivet om nät- och informationssäkerhet och med Europols europeiska centrum mot it-brottslighet, Cert-EU och relevanta brottsbekämpande organ.

Ett informationsutbyte mellan aktörer och myndigheter under cyberriskernas hela livscykel förutsätter att deltagarna känner förtroende för att detta inte kommer att utsätta dem för några ansvarsrisker. Kommissionen har noterat ett antal sådana farhågor som hindrar företagen från att utbyta värdefull information om hot med sina motsvarigheter inom andra sektorer eller med myndigheter, särskilt över gränserna. Kommissionen kommer att sträva efter att bemöta och minska dessa farhågor för att därigenom förbättra informationsutbytet om cyberhot.

Tillförlitliga rapporteringskanaler som garanterar konfidentialiteten är också viktiga för att uppmuntra företagen att rapportera om cyberstölder av företagshemligheter. Detta skulle göra det möjligt att övervaka och bedöma den skada som åsamkas det europeiska näringslivet (som också medför en minskad försäljning och förlorade arbetstillfällen) och forskningsorganen. Det skulle också bidra till fastställandet av en ändamålsenlig politik. Med stöd av Enisa, Europeiska unionens immaterialrättsmyndighet (EUIPO) och EC3 vid Europol och i dialog med privata intressenter kommer kommissionen att inrätta tillförlitliga kanaler för frivillig rapportering av cyberstöld av företagshemligheter. Detta bör göra det möjligt att sammanställa anonymiserade och aggregerade uppgifter på EU-nivå. Dessa uppgifter kan utbytas med medlemsstaterna och användas som underlag för diplomatiska insatser och informationsåtgärder som kan bidra till att skydda EU:s immateriella tillgångar från cyberattacker.

För att främja cybersäkerheten inom olika sektorer kommer kommissionen också att verka för att cybersäkerhetsaspekterna beaktas vid utarbetandet av EU-politiken för olika sektorer där cybersäkerheten spelar en avgörande roll.

---

[19] SWD(2013) 318.

[20] T.ex. Europeiska byrån för luftfartssäkerhets plan för cybersäkerhet och cybersäkerhetsarbetet inom Internationella civila luftfartsorganisationen och Internationella sjöfartsorganisationen.

[21] Se t.ex. ISAC-centrumet för europeisk energi (http://www.ee-isac.eu).

Sist men inte minst har offentliga organ en viktig funktion när det gäller kontrollen av integriteten för viktiga internetinfrastrukturer för att upptäcka problem, informera den part som ansvarar för dessa nät och – vid behov – erbjuda bistånd med att åtgärda kända svaga punkter. De nationella regleringsmyndigheterna skulle kunna använda CSIRT-kapacitet för att göra regelbundna avsökningar av offentliga nätinfrastrukturer. På denna grundval kan de sedan uppmuntra operatörer att åtgärda luckor eller svaga punkter som identifieras i avsökningarna.

Kommissionen kommer därför att undersöka vilka rättsliga och organisatoriska villkor som behövs för att de nationella regleringsmyndigheterna – i samarbete med nationella cybersäkerhetsmyndigheter – ska kunna begära att CSIRT-nätverken utför regelbundna sårbarhetskontroller av offentlig nätinfrastrukturer. Nationella CSIRT-enheter bör uppmuntras att samarbeta inom CSIRT-nätverket om bästa praxis för övervakning av nät, för att på så sätt göra det lättare att förebygga storskaliga incidenter.

Kommissionen kommer att göra följande:

- Främja utvecklingen av ett europeiskt samarbete mellan sektorsvisa centrum för informationsutbyte och analys, stödja deras samverkan med CSIRT-enheter och verka för att undanröja sådant som hindrar marknadsaktörerna från att utbyta information.
- Studera de strategiska riskerna och systemriskerna på grund av cyberincidenter inom sektorer med stort ömsesidigt beroende inom och över nationella gränser.
- Bedöma behovet av och, om lämpligt, överväga ytterligare bestämmelser och/eller vägledning om cyberriskberedskap inom kritiska sektorer.
- Tillsammans med Enisa, EUIPO och EC3 upprätta tillförlitliga kanaler för frivillig rapportering om cyberstöld av företagshemligheter.
- Främja en integrering av cybersäkerhetsåtgärder inom den europeiska politiken för olika sektorer.
- Granska vilka villkor som krävs för att de nationella myndigheterna ska kunna begära att CSIRT-enheter utför regelbundna kontroller av viktig nätinfrastruktur.

3. HUR SKA UTMANINGARNA PÅ EUROPAS INRE MARKNAD FÖR CYBERSÄKERHET BEMÖTAS?

Europa behöver billiga och interoperabla cybersäkerhetsprodukter och cybersäkerhetslösningar av hög kvalitet. Tillgången på IKT-säkerhetsprodukter och -tjänster på den inre marknaden är fortfarande mycket fragmenterad geografiskt sett. Detta gör det svårt för de europeiska företagen att konkurrera på nationell, europeisk och global nivå. Det minskar också utbudet av fungerande och användbar cybersäkerhetsteknik som medborgarna och företagen får tillgång till[22].

Cybersäkerhetsbranschen i Europa har i princip utvecklats på grundval av nationell statlig efterfrågan, bland annat från försvarssektorn. De flesta europeiska leverantörer av

[22] Se SWD(2016) 216.

försvarsmateriel har utvecklat cybersäkerhetsenheter[23]. Samtidigt har en mängd innovativa små och medelstora företag vuxit fram på både specialiserade marknader och nischmarknader (t.ex. krypteringssystem) och på etablerade marknader med nya affärsmodeller (t.ex. antivirusprogram).

Företagen har dock haft svårt att växa utanför sin egen nationella marknad. Bristen på förtroende för de lösningar som erbjuds över gränserna är en viktig faktor, vilket framgick tydligt av det samråd som genomfördes av kommissionen[24]. Följaktligen sker mycket upphandling fortfarande inom enskilda medlemsstater, och många företag kämpar för att uppnå de stordriftsfördelar som skulle kunna göra dem mer konkurrenskraftiga både på den inre marknaden och globalt.

Bristen på interoperabla lösningar (tekniska standarder), förfaranden (processtandarder) och EU-mekanismer för certifiering är några faktorer som påverkar den inre marknaden för cybersäkerhet. Cybersäkerheten angavs också som ett prioriterat område för IKT-standardisering på den digitala inre marknaden[25].

Cybersäkerhetsföretagens begränsade utsikter för tillväxt på den inre marknaden leder till många fusioner och uppköp som görs av icke-europeiska investerare[26]. Denna trend visar innovationskraften hos de europeiska cybersäkerhetsentreprenörerna, men samtidigt riskerar den att leda till förlust av kunnande och expertis i Europa och till en kompetensflykt.

Brådskande åtgärder behövs för att främja en mer integrerad inre marknad för cybersäkerhetsprodukter och -tjänster som kommer att underlätta införandet av mer praktiska och överkomliga lösningar.

Förtroendehindren mellan europeiska industriaktörer och institutionella aktörer kan undanröjas om man främjar ett samarbete i en tidig fas av innovationens livscykel: inom själva cybersäkerhetsbranschen och mellan leverantörer och köpare, och i en sektorsövergripande dimension som involverar företag som redan är eller sannolikt kommer att bli kunder när det gällercybersäkerhetslösningar.

Samtidigt kommer utvecklingen av produkter, tjänster och teknik med dubbla användningsområden att bli allt viktigare i Europa. Allt fler lösningar från den civila marknaden börjar användas på försvarsmarknaden[27]. I den kommande europeiska handlingsplanen på försvarsområdet kommer kommissionen att ange åtgärder som ytterligare kan stärka de civil-militära synergierna på europeisk nivå.

3.1 Certifiering och märkning

Certifiering är mycket viktig för att öka förtroendet och säkerheten när det gäller varor och tjänster. Detta gäller också för de nya system som i hög grad bygger på digital teknik och som kräver en hög säkerhetsnivå, såsom uppkopplade och automatiserade bilar, elektronisk hälsovård, industriella automatiseringskontrollsystem (IACS) eller smarta elnät.

[23] Se SWD(2016) 216.
[24] Se SWD(2016) 215.
[25] COM(2016) 176 final, s. 2.
[26] Se SWD(2016) 216.
[27] 2013 utgjorde export med dubbla användningsområden omkring 20 % av EU:s totala export (i värde). Siffran inkluderar handel inom EU.

Nationella initiativ har inletts för att fastställa högt ställda cybersäkerhetskrav för IKT-komponenter i traditionell infrastruktur, inbegripet certifieringskrav. Dessa är viktiga, men riskerar att medföra fragmentering på den inre marknaden och skapa interoperabilitetsproblem. Endast i ett fåtal medlemsstater finns det effektiva säkerhetscertifieringssystem för IKT-produkter[28]. En IKT-säljare kan därför behöva genomgå flera certifieringsprocesser för att kunna sälja i flera medlemsstater. I värsta fall kan det hända att en IKT-produkt eller IKT-tjänst som utformats för att uppfylla cybersäkerhetskrav i en medlemsstat inte får släppas ut på marknaden i en annan medlemsstat.

För att skapa en fungerande inre marknad för cybersäkerhet bör en eventuell ram för säkerhetscertifiering av IKT-produkter och IKT-tjänster sikta på i) att omfatta många olika typer av IKT-system, IKT-produkter och IKT-tjänster, ii) att säkerställa tillämpning i samtliga 28 medlemsstater, och iii) att omfatta varje cybersäkerhetsnivå. Samtidigt måste hänsyn tas till den internationella utvecklingen.

För detta ändamål kommer kommissionen att inrätta en särskild arbetsgrupp för säkerhetscertifiering av IKT-produkter och IKT-tjänster, bestående av experter från medlemsstaterna och näringslivet. Syftet är att i samarbete med Enisa och gemensamma forskningscentrumet före utgången av 2016 ta fram en färdplan för att undersöka möjligheten att lägga fram ett förslag till en sådan europeisk IKT-säkerhetscertifieringsram före utgången av 2017. I detta sammanhang kommer kommissionen även att beakta förordning (EG) nr 2008/765 och certifieringsbestämmelserna i den allmänna dataskyddsförordningen nr 2016/679[29].

Processen kommer att omfatta ett brett samråd och en konsekvensbedömning. Det här kommer att göra det möjligt för kommissionen att undersöka olika alternativ för inrättandet av en certifieringsram för IKT-produkter och IKT-tjänster. Kommissionen kommer också att granska IKT-säkerhetscertifieringen inom infrastruktursektorer (t.ex. inom luftfart, järnväg, fordon) samt inom specifika certifierings- och valideringsmekanismer för teknik som är färdig att börja användas (t.ex. cybersäkerhet för industriella automatiseringskontrollsystem[30], sakernas internet, molntjänster). Kommissionen kommer också att åtgärda konstaterade brister inom ovannämnda IKT-säkerhetscertifieringssystem.

I möjligaste mån kommer certifieringsarbetet att baseras på internationellt erkända standarder och utvecklas tillsammans med internationella partner.

Kommissionen kommer också att undersöka olika alternativ för hur man bäst kan beakta IKT-säkerhetscertifiering i framtida sektorsspecifik lagstiftning, som också avser säkerhetsaspekter.

---

[28] Se SWD(2016) 216 för överenskommelsen i chefstjänstemännens grupp för informationssystem (rådets beslut av den 31 mars 1992 (92/242/EEG)) och andra befintliga system som t.ex. Commercial Product Assurance i Förenade kungariket och Certification Sécuritaire de Premier Niveau i Frankrike.

[29] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter omfattar såväl uppförandekoder som ska bidra till en korrekt tillämpning av dataskyddsbestämmelserna som certifieringsmekanismer som omfattar alla dataskyddsprinciper, bl.a. dataskydd vid hantering av personuppgifter.

[30] Se Erncips temagrupp ”Cyber security of Industrial Control Systems”, på https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

Förutom möjliga lagstiftningsalternativ kommer kommissionen också att undersöka möjligheten att införa ett europeiskt, kommersiellt inriktat, frivilligt och enkelt märkningssystem för säkerheten i IKT-produkter. Märkningssystemet skulle komplettera certifieringen och syfta till att öka läsbarheten för cybersäkerheten i kommersiella produkter för att på så sätt öka deras konkurrenskraft på den inre marknaden och globalt. Vederbörlig hänsyn kommer att tas till pågående sektoriella och övergripande initiativ från branschen, på både utbuds- och efterfrågesidan.

Offentliga förvaltningar kommer att engageras för att främja användning av gemensamma specifikationer och hänvisning till certifiering vid offentlig upphandling. Kommissionen kommer också att övervaka och rapportera om användningen av relevanta certifieringskrav inom offentlig upphandling på nationell nivå, särskilt när det gäller sektorspecifika system (t.ex. energi, transport, hälso- och sjukvård och offentlig förvaltning).

Kommissionen kommer att göra följande:

- Före utgången av 2016 utarbeta en färdplan mot en eventuell europeisk IKT-säkerhetscertifieringsram, som bör läggas fram senast i slutet av 2017, och bedöma genomförbarheten för och konsekvenserna av en enkel europeisk ram för cybersäkerhetsmärkning.
- Undersöka behovet av och, i förekommande fall, åtgärda brister när det gäller IKT-säkerhetscertifiering inom befintliga sektorsspecifika mekanismer för certifiering och validering.
- När så är lämpligt ta med IKT-produktsäkerhetscertifiering i framtida sektorsspecifika lagstiftningsförslag.
- Engagera offentliga organ i att främja användningen av certifiering och gemensamma specifikationer vid offentlig upphandling.
- Övervaka användningen av relevanta certifieringskrav för offentlig och privat upphandling och rapportera om marknadssituationen om tre år.

3.2. Öka investeringarna i cybersäkerhet i Europa och stödja små och medelstora företag

Det pågår ett intensivt innovationsarbete i den europeiska cybersäkerhetssektorn, men EU saknar fortfarande en stark kultur för investering i cybersäkerhet. Det finns många innovativa små och medelstora företag på området, men de kan ofta inte bygga ut sin verksamhet. Detta beror bland annat på bristen på lättillgänglig finansiering för att klara de tidiga utvecklingsfaserna. Företagen har också begränsad tillgång till riskkapital i Europa, och deras budget är inte tillräcklig för att täcka den marknadsföring de behöver för att öka sin synlighet eller för att klara olika uppsättningar av standarder och krav.

Samtidigt samarbetar cybersäkerhetsaktörerna endast på enstaka områden, och ytterligare insatser krävs för att öka den ekonomiska koncentrationen och utveckla nya värdekedjor[31].

Om vi ska kunna öka investeringarna i europeisk cybersäkerhet och stödja små och medelstora företag, är det nödvändigt att underlätta tillgången till finansiering. Det måste också finnas ett stöd för utvecklingen av globalt konkurrenskraftiga cybersäkerhetskluster och spetsforskningscentrum inom gynnsamma regionala ekosystem för digital tillväxt. Detta stöd behöver kopplas till genomförandet av smarta specialiseringsstrategier och andra EU-instrument så att den europeiska cybersäkerhetsindustrin utnyttjar dem bättre.

Kommissionens kommer att arbeta för att maximera cybersäkerhetsbranschens medvetenhet om finansieringsmöjligheterna på europeisk, nationell och regional nivå (både övergripande instrument och särskilda ansökningsomgångar[32]) genom att använda befintliga instrument och kanaler som Enterprise Europe Network.

Kommissionen kommer att komplettera dessa insatser genom att tillsammans med Europeiska investeringsbanken (EIB) och Europeiska investeringsfonden (EIF) undersöka hur man kan underlätta tillgången till finansiering. Detta kan ske i form av kapitalinvestering eller investering i form av kapital likställt med eget kapital, lån, garantier för projekt eller motgarantier till intermediärer, t.ex. genom inrättandet av en investeringsplattform för cybersäkerhet inom Europeiska fonden för strategiska investeringar[33].

Kommissionen kommer också tillsammans med berörda medlemsstater och regioner att titta på möjligheten att inrätta en cybersäkerhetsplattform för smart specialisering[34]. Detta skulle underlätta samordning och planering av cybersäkerhetsstrategier och upprätta strategisk samverkan mellan berörda parter i regionala ekosystem. På så sätt kan man bidra till att frigöra de europeiska struktur- och investeringsfondernas potential för cybersäkerhetssektorn.

Mer allmänt kommer kommissionen att främja en syn präglad av *security-by-design*. Den kommer att verka för att cybersäkerhetskrav beaktas på ett konsekvent sätt i alla större infrastrukturinvesteringar som har en digital komponent och som medfinansieras av de europeiska fonderna. Därför kommer den att gradvis införa relevanta krav i bestämmelser för offentlig upphandling och programbestämmelser.

Kommissionen kommer att göra följande:

- Använda befintliga verktyg för stöd till små och medelstora företag för att öka

[31] Se SWD(2016) 216.

[32] Se t.ex. 2016 års sektorsövergripande ansökningsomgång inom Fonden för ett sammanlänkat Europa och 2016 års Cosmo-ansökningsomgångar avseende programmet för internationalisering av kluster

[33] Inom ramen för Europeiska fonden för strategiska investeringar kan enskilda projekt stödjas antingen direkt eller indirekt genom investeringsplattformar. Sådana plattformar kan bidra till finansieringen av mindre projekt och slå ihop finansiering från olika källor för att möjliggöra diversifierade investeringar med geografisk eller tematisk inriktning.

[34] Se instrument för smart specialisering (RIS3): http://s3platform.jrc.ec.europa.eu/.

kunskaperna om befintliga finansieringsmekanismer bland cybersäkerhetsaktörer.
- Ytterligare öka användningen av EU-verktyg och EU-instrument för att hjälpa innovativa små och medelstora företag att hitta synergier mellan de civila och militära cybersäkerhetsmarknaderna[35].
- Tillsammans med EIB och EIF undersöka möjligheterna att förenkla tillgången till investeringar, t.ex. genom en särskild investeringsplattform för cybersäkerhet eller andra verktyg.
- Utveckla en cybersäkerhetsplattform för smart specialisering för att hjälpa medlemsstater och regioner som är intresserade av att investera i cybersäkerhet (RIS3).
- Främja *security-by-design* vid stora infrastrukturinvesteringar som har en digital komponent och som medfinansieras av EU-fonder.

4. FRÄMJA DEN EUROPEISKA CYBERSÄKERHETSBRANSCHEN GENOM INNOVATION – INRÄTTANDE AV OFFENTLIG-PRIVATA CYBERSÄKERHETSPARTNERSKAP

För att främja konkurrenskraft och innovation för den europeiska cybersäkerhetsbranschen kommer ett avtal om ett offentlig-privat cybersäkerhetspartnerskap att undertecknas. Cybersäkerhetspartnerskapet kommer att samla företagsresurser och offentliga resurser för att uppnå spetskompetens inom forskning och innovation.

Partnerskapet syftar till att öka förtroendet mellan medlemsstaterna och aktörerna inom näringslivet genom att främja samarbete i ett tidigt skede av forsknings- och innovationsprocessen. Det syftar också till att bidra till att jämka samman utbuds- och efterfrågesektorerna. Detta bör göra det möjligt för industrin att få grepp om framtida krav från slutanvändarna och de sektorer som är viktiga kunder när det gäller cybersäkerhetslösningar (t.ex. energi, hälso- och sjukvård, transport och finans), vi vilket kommer att underlätta deras deltagande i fastställandet av gemensamma krav för digital säkerhet och dataskydd inom sina sektorer.

Det offentlig-privata cybersäkerhetspartnerskapet kommer också att bidra till att användningen av tillgängliga medel maximeras. Detta kommer att uppnås främst genom en ökad samordning med medlemsstaterna. Det kommer också att öka fokuseringen på några få tekniska prioriteringar för att hjälpa cybersäkerhetsbranschen att göra tekniska genombrott och behärska viktig framtidsteknik för cybersäkerhet. I detta sammanhang kan utvecklingen av öppen programvara och öppna standarder bidra till att främja förtroende, öppenhet och banbrytande innovationer, och därför bör även sådant omfattas av investeringarna inom det offentlig-privata cybersäkerhetspartnerskapet.

Det arbete som görs inom partnerskapet kommer också att korsbefruktas av andra europeiska projekt, i synnerhet sådana som behandlar säkerhetsaspekter. Hit hör offentlig-privata

[35] T.ex. Enterprise Europe Network och det europeiska nätverket av regioner med försvarsanknytning (European Network of Defence-related Regions) kommer att ge regionerna nya möjligheter att undersöka gränsöverskridande samarbete avseende dubbla användningsområden, inklusive cybersäkerhet, och små och medelstora företag möjlighet att delta i kontaktskapande verksamhet.

partnerskap avseende fabriker för framtiden, energieffektiva byggnader, 5G och stordata[36], andra offentlig-privata partnerskap inom olika sektorer[37] samt initiativet för sakernas internet[38]. Dessutom kommer man att främja en långtgående anpassning till det europeiska öppna forskningsmolnet och det europeiska superdatorinitiativet för kvantteknik på cyberområdet (dvs. innovation inom kvantnyckeldistribution och forskning om kvantdatorteknik).

Det offentlig-privata partnerskapet för cybersäkerhet inleds inom ramen för Horisont 2020[39], EU:s ramprogram för forskning och innovation för perioden 2014–2020. Det kommer att mobilisera medel från två av programmets pelare: Ledarskap inom möjliggörande teknik och industriteknik (LEIT-ICT) och Samhällsutmaning – Säkra samhällen (SC7). Partnerskapet kommer att ha en total budget på 450 miljoner euro, där en tredubbel hävstångsfaktor väntas från branschens sida. Cybersäkerheten bör också behandlas i och samordnas med andra relevanta delar av Horisont 2020 (t.ex. samhällsutmaningar avseende energi, transport och hälso- och sjukvård samt spetskompetensdelen inom Horisont 2020). Detta kommer att bidra till målen för det offentlig-privata partnerskapet för cybersäkerhet. Samordning bör ske redan vid utarbetandet av sektorsvisa strategier.

Det offentlig-privata partnerskapet kommer att genomföras på ett öppet sätt och med öppna och flexibla styrelseformer som är anpassade till cybersäkerhetsvillkorens snabba utveckling. Det kommer att beakta medlemsstaternas behov av att diskutera hur teknikutvecklingen påverkar möjligheterna till säker drift av nationella och gränsöverskridande infrastrukturer. Partnerskapet måste leda till resultat som håller i flera år för att säkerställa att målen ska kunna uppnås.

Partnerskapet kommer att stödjas av Ecso (den europeiska cybersäkerhetsorganisationen), vars sammansättning kommer att återspegla den europeiska cybersäkerhetsmarknadens mångfald. Det kommer även att omfatta nationella, regionala och lokala offentliga förvaltningar, forskningscentrum, den akademiska världen och andra berörda parter.

Kommissionen kommer att göra följande:

- Underteckna ett avtal med branschen om ett offentlig-privat partnerskap för cybersäkerhet, så att arbetet kan inledas under det tredje kvartalet 2016.
- Inleda Horisont 2020-ansökningsomgångarna för det offentlig-privata partnerskapet under första kvartalet 2017.
- Samordna det offentlig-privata partnerskapet med relevanta sektorsstrategier, Horisont 2020-instrument och offentlig-privata partnerskap inom andra sektorer.

5. SLUTSATS

I detta meddelande redogörs för åtgärder som syftar till att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch i Europa,

[36] Det offentlig-privata partnerskapet för 5G-infrastruktur och det offentlig-privata partnerskapet Big Data Value.
[37] T.ex. det offentlig-privata partnerskapet Sesar eller Shift2Rail.
[38] The Alliance for Internet of Things Innovation (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

såsom aviseras i EU-strategin för cybersäkerhet och strategin för den digitala inre marknaden. Kommissionen uppmanar Europaparlamentet och rådet att stödja rapporten.