Europeiska kommissionen

TILLSTÅNDET I UNIONEN 2018

Stark cybersäkerhet i Europa

#SOTEU

12 september 2018

”Cyberattacker respekterar inga gränser, men vår förmåga att hantera dem varierar kraftigt från ett land till ett annat, vilket skapar kryphål och sårbarheter som lockar till sig ännu fler attacker. EU behöver mer robusta och effektiva strukturer för att säkra en stark cyberresiliens och hantera cyberattacker. Vi vill inte vara de svagaste länkarna när det gäller detta globala hot.”

Jean-Claude Juncker, det digitala toppmötet i Tallinn, 29 september 2017

Europeiska kommissionen och den höga representanten lade 2017 fram en rad olika åtgärder för att bygga upp en stark cybersäkerhet och ge Europa verktyg att hantera ett cyberhot som hela tiden förändras. Nu kompletteras dessa åtgärder med ett förslag som ska göra det lättare för EU att samla sina resurser och sin expertis inom forskning och innovation och gå i bräschen för nästa generation cybersäkerhetsteknik och digitala teknik.

Dagens cyberhot

Under 2016 inträffade **mer än 4 000 ransomwareattacker** om dagen

80 % av alla europeiska företag drabbades av minst en cybersäkerhetsincident förra året

Antalet **säkerhetsincidenter ökade med 38 %** inom alla branscher, vilket var den största ökningen på tolv år

I en del medlemsstater är **50 % av alla brott** cyberbrott

Mer än 150 länder och mer än 230 000 system i olika sektorer och länder drabbades av Wannycry-attacken i maj 2017, och den hade stor inverkan på grundläggande samhällsservice som är kopplad till internet, däribland sjukhus och ambulanstjänster

Starkare förmåga att stå emot cyberattacker

Kommissionen ger redan stöd för att stärka EU:s förmåga att avskräcka, stå emot och hantera cyberattacker. Det sker bl.a. genom

stöd till genomförandet av EU:s första cybersäkerhetsakt (direktivet om säkerhet i nätverks- och informationssystem) genom

STÖRRE KAPACITET

Medlemsstaterna måste förbättra sin kapacitet när det gäller cybersäkerhet

SAMARBETE

Ökat samarbete på EU-nivå

RISKFÖREBYGGANDE

Aktörer inom viktiga sektorer (som energi, transport och hälsa) är skyldiga att vidta åtgärder för att förebygga risker och hantera cyberincidenter

Samarbete med EU-länderna kring

EU: S CYBERSÄKERHETSBYRÅ

Stärka Europeiska unionens cybersäkerhetsbyrå så att den kan bistå medlemsstaterna på ett bättre sätt

EU-REGELVERK FÖR CERTIFIERING

Ett EU-regelverk för certifiering för att säkerställa att produkter och tjänster är cybersäkra

SAMORDNAD HANTERING AV ATTACKER

Snabb och samordnad hantering av storskaliga cyberattacker

Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) bistår medlemsstaternas cybersäkerhetsmyndigheter för att stärka EU:s skydd mot cyberattacker.

Samla resurser och expertis inom cybersäkerhetsteknik

I dag föreslår kommissionen att man utöver de cybersäkerhetsinitiativ som redan finns i EU även ska etablera ett nätverk av kompetenscentrum och inrätta ett europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning. Syftet är att främja utveckling och införande av de verktyg och den teknik som behövs för att hålla jämna steg med ett cyberhot som hela tiden förändras.

Det europeiska kompetenscentrumet ska tillsammans med medlemsstaterna på ett så målinriktat sätt som möjligt samordna de medel som avsatts för cybersäkerhet i EU:s nästa långtidsbudget. Detta kommer att skapa ny cyberkapacitet inom EU.

Det finns redan en mängd kunskap inom EU, som har mer än **660 kompetenscentrum på cybersäkerhetsområdet**. För att man ska kunna ta tillvara och utnyttja denna kunskap på ett effektivt sätt föreslår kommissionen att det införs en mekanism för att

slå ihop, utbyta och ge tillgång till befintlig expertis

främja införandet av cybersäkerhetsprodukter och lösningar

säkerställa ett långsiktigt strategiskt samarbete mellan företag, forskarsamhällen och stater

göra gemensamma investeringar och dela kostsam infrastruktur

Europeiska kompetenscentrumet:

Ska samordna användningen av medel för cybersäkerhet som avsatts i EU:s nästa långtidsbudget (2021–2027) i programmen Ett digitalt Europa och Horisont Europa. Kompetenscentrumet ska hjälpa kompetensnätverket och kompetensgemenskapen att driva **cybersäkerhetsagendan** när det gäller forskning och innovation. Det ska även organisera **gemensamma investeringar** av EU, medlemsstaterna och näringslivet. Programmet Ett digitalt Europa ska t.ex. satsa **2 miljarder euro** på att skydda EU:s digitala ekonomi, samhälle och demokrati genom stöd till EU-företag som är verksamma inom cybersäkerhet samt finansiering av avancerad cybersäkerhetsutrustning och infrastruktur.

Nätverket av nationella samordningscentrum:

Varje medlemsstat ska utse ett nationellt samordningscentrum till nätverket som ska ägna sig åt utveckling av cybersäkerhetskapacitet och mer övergripande kompetensutveckling. Nätverket ska bidra till att kartlägga och stödja de mest relevanta cybersäkerhetsprojekten i medlemsstaterna.

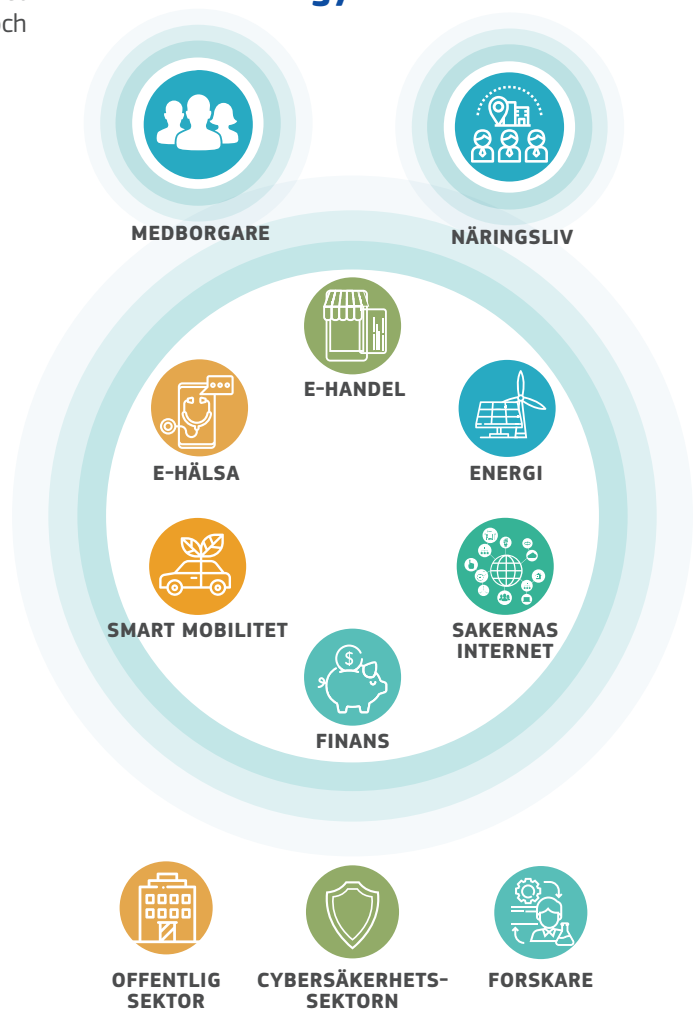
Kompetensgemenskapen:

En stor, öppen och mångskiftande grupp aktörer inom cybersäkerhet från forskarsamhället och privat och offentlig sektor, samt civila och försvarsrelaterade myndigheter.

Vad kommer att bli bättre?

- Bättre samordning av arbetet
- Tillgång till expertis
- Tillgång till test- och försöksanläggningar
- Bedömning av produkters cybersäkerhet
- Tillgång till innovativa cybersäkerhetsprodukter och lösningar
- Främjande av marknadens upptag av produkter och tjänster
- Ökad synlighet mot potentiella investerare och affärspartner
- Lägre kostnader tack vare gemensamma investeringar med andra medlemsstater
- EU får förmåga att själv säkra sin ekonomi och demokrati
- EU blir världsledande inom cybersäkerhet

Vem kommer detta att gynna?



Publikationsbyrån

Print ISBN 978-92-79-92499-6 doi:10.2775/086133 NA-04-18-693-SV-C
PDF ISBN 978-92-79-92460-6 doi:10.2775/249475 NA-04-18-693-SV-N