Unionens tilstand 2017 - Cybersikkerhed Kommissionen intensiverer EU's indsats over for cyberangreb

Bruxelles, den 19. september 2017

.

I sin årlige tale om Unionens tilstand den 13. september udtalte **EU-formand Jean-Claude Juncker**: "*Vi har i de sidste tre år gjort fremskridt med at sørge for, at europæerne kan færdes sikkert online. Europa er imidlertid stadig ikke godt rustet mod cyberangreb. Derfor fremsætter Kommissionen i dag forslag til nye værktøjer, herunder et EU-agentur for cybersikkerhed, der skal bidrage til at forsvare os mod sådanne angreb.*"

Europæerne sætter stor lid til de digitale teknologier. Disse teknologier skaber nye muligheder for kontakt mellem borgerne, letter informationsformidlingen og udgør rygraden i Europas økonomi. De medfører imidlertid også nye risici, idet både ikkestatslige og statslige aktører i stigende grad forsøger at stjæle oplysninger, begå svig og endog destabilisere regeringer. Sidste år var der dagligt mere end 4 000 afpresningssoftwareangreb i Europa, og 80 % af de europæiske virksomheder var ude for mindst én cybersikkerhedshændelse. Økonomiske tab som følge cyberkriminalitet er i de seneste fire år alene steget til det femdobbelte.

Med henblik på at udstyre Europa med de rette værktøjer til at imødegå cyberangreb har Europa-Kommissionen og den højtstående repræsentant fremsat forslag til en lang række foranstaltninger, der skal styrke cybersikkerheden i EU. Dette omfatter et forslag til et nyt **EU-agentur for cybersikkerhed**, der skal bistå medlemsstaterne i deres håndtering af cyberangreb, samt en ny **europæisk certificeringsordning**, som vil sikre, at det er sikkert at benytte produkter og tjenester i den digitale verden.

Federica **Mogherini**, højtstående repræsentant og næstformand, udtaler: "*EU vil forfølge en international cyberpolitik, der lægger vægt på et åbent, frit og sikkert cyberspace, og som støtter bestræbelserne på at udvikle normer for ansvarlig statslig adfærd, på at anvende folkeretten samt på at fremme tillidsskabende foranstaltninger vedrørende cybersikkerhed.*"

Andrus **Ansip**, næstformand med ansvar for det digitale indre marked, udtaler: *"Intet land kan imødegå cybersikkerhedsmæssige udfordringer alene. Vores initiativer styrker samarbejdet mellem EU's medlemsstater, så de sammen kan tackle disse udfordringer. Vi har også fremsat forslag til nye foranstaltninger, der skal booste investeringer i innovation og fremme cyberhygiejne."*

Julian **King**, EU-kommissær med ansvar for sikkerhedsunionen, udtaler: "*Vi er med henblik på at styrke vores fælles* cybersikkerhed nødt til at samarbejde om at opbygge vores modstandsdygtighed, fremme foranstaltninger med afskrækkende virkning, styrke sporing og ansvarlighed samt fremme samarbejde på internationalt plan."

Mariya **Gabriel**, kommissær med ansvar for den digitale økonomi, udtaler: *"Vi skal bygge videre på den tillid vores borgere og virksomhederne har til den digitale verden, især i en tid hvor omfattende cyberangreb bliver mere og mere almindelige. Det er mit ønske, at høje cybersikkerhedsstandarder bliver den nye konkurrencemæssige fordel, der kendetegner vores virksomheder."*

I lyset af de seneste afpresningssoftwareangreb, en dramatisk stigning i cyberkriminalitet, statslige aktørers øgede anvendelse af cyberværktøjer til opnåelsen af deres geopolitiske mål samt den stigende variation i typen af cybersikkerhedshændelser har EU behov for at opbygge større modstandsdygtighed over for cyberangreb og etablere et effektivt EU-dækkende cyberforsvar, der har afskrækkende virkning samt effektiv strafferetlig forfølgning for bedre at beskytte EU's borgere, virksomheder og offentlige institutioner. Det er dét pakken for cybersikkerhed, der præsenteres i dag, handler om.

Styrkelse af EU's modstandsdygtighed: Et solidt EU-agentur for cybersikkerhed

Et EU-agentur for cybersikkerhed Agenturet bygger videre på det eksisterende Europæiske Agentur for Netværks- og Informationssikkerhed (ENISA) og vil få permanent mandat til at bistå medlemsstaterne i deres bestræbelser på effektivt at reagere på og bekæmpe cyberangreb. Agenturet vil forbedre EU's beredskab ved at organisere årlige **fælleseuropæiske cybersikkerhedsøvelser** og sikre bedre **udveksling af efterretningsoplysninger om trusler** gennem oprettelsen af centre til informationsudveksling og -analyse. Det vil fremme gennemførelsen af **direktivet om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer**, der omfatter en rapporteringsforpligtelse for de nationale myndigheder i tilfælde af alvorlige hændelser.

Agenturet for cybersikkerhed vil også bidrage til at indføre og gennemføre den **EU-dækkende certificeringsramme**, som Kommissionen har foreslået med henblik på at sikre **cybersikre produkter og tjenester**. Forbrugerne kan takket være EU's fødevaremærkning have tillid til de produkter, de spiser, og de nye europæiske cybersikkerhedscertifikater vil på samme vis sikre pålideligheden af de milliarder af apparater ("tingenes internet"), der understøtter vore dages kritiske infrastrukturer, såsom energi- og transportnetværk, men også nye forbrugerprodukter, som f.eks. internetforbundne biler. Cybersikkerhedscertifikater vil blive anerkendt på tværs af medlemsstaterne, og vil dermed mindske virksomhedernes administrative byrde og omkostninger[1].

Styrkelse af EU's cybersikkerhedskapacitet

Det er i EU's strategiske interesse at sikre, at de teknologiske værkstøjer på cybersikkerhedsområdet udvikles på en måde, der fremmer den digitale økonomi, samtidig med at vores sikkerhed, samfund og demokrati beskyttes. Dette omfatter også beskyttelsen af kritisk IT-hardware og -software. Med henblik på at styrke EU's cybersikkerhedskapacitet foreslår Kommissionen og den højtstående repræsentant:

- **Et europæisk forsknings- og videnscenter for cybersikkerhed** (et pilotprogram, der vil blive etableret i løbet af 2018). Det vil i samarbejde med medlemsstaterne bidrage til at udvikle og indføre de værktøjer og den teknologi, der er nødvendig for at tackle en konstant skiftende trussel, samt sikre, at vores forsvar er ligeså avanceret som de våben cyberkriminelle anvender. Det vil endvidere supplere kapacitetsopbygningsindsatsen på dette område i EU og på nationalt plan
- En vejledende plan for, hvordan EU og medlemsstaterne hurtigt, i praksis og i fælleskab **kan reagere** på et omfattende cyberangreb. Den foreslåede procedure er fastlagt i en henstilling, som blev vedtaget i sidste uge. I henstillingen anmodes medlemsstaterne og EU-institutionerne desuden om at etablere en EU-kriseberedskabsramme for cybersikkerhed med henblik på at gøre den vejledende plan operationel. Den vil blive testet regelmæssigt i forbindelse med cyberberedskabsøvelser og andre krisestyringsøvelser
- **Øget solidaritet**: Det kan i fremtiden overvejes at oprette en ny nødhjælpsfond for cybersikkerhed for de medlemsstater, som på ansvarlig vis har gennemført alle de sikkerhedsforanstaltninger, der er påkrævet i henhold til EU-lovgivningen. Fonden kan yde nødhjælp med henblik på at bistå medlemsstaterne, ligesom EU's civilbeskyttelsesordning anvendes i tilfælde af skovbrande eller naturkatastrofer
- **En styrket cyberforsvarskapacitet**: For at støtte cyberforsvarsprojekter tilskyndes medlemsstaterne til at inkludere cyberforsvar i det arbejde, der pågår inden for rammerne af det permanente strukturerede samarbejde (PESCO) og den europæiske forsvarsfond. Det europæiske forsknings- og videnscenter for cybersikkerhed kunne også videreudvikles med en cyberforsvarsdimension. For at imødegå kvalifikationskløften inden for cyberforsvar vil EU i 2018 oprette en trænings- og uddannelsesplatform for cyberforsvar. EU og NATO vil sammen fremme samarbejde om forskning og innovation i cyberforsvar. Samarbejdet med NATO vil blive intensiveret, herunder ved deltagelse i parallelle og koordinerede øvelser
- **Øget internationalt samarbejde**: Ved at gennemføre rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter vil EU styrke sin indsats over for cyberangreb og støtte en strategisk ramme til konfliktforebyggelse og stabilitet i cyberspace. Dette vil blive ledsaget af cyberkapacitetsopbyggende foranstaltninger, der skal hjælpe tredjelande med at imødegå cybertrusler.

Effektiv strafferetlig indsats

En mere effektiv strafferetlig indsats med fokus på afsløring, sporing og retsforfølgning af cyberkriminelle spiller en central rolle for opbyningen af et effektivt cyberforsvar, der også har afskrækkende virkning. Kommissionen foreslår derfor at booste denne afskrækkende virkning ved

hjælp af nye foranstaltninger til **bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter**.

Det foreslåede **direktiv** vil styrke de retshåndhævende myndigheders kapacitet til at håndtere denne form for kriminalitet ved at **udvide omfanget af handlinger, som er strafbare**, og som er relateret til informationssystemer til at omfatte alle betalingstransaktioner, herunder transaktioner foretaget ved hjælp af elektroniske omsætningsmidler. Denne lovgivning vil endvidere indføre **fælles regler om sanktionsniveauer** samt præcisere **medlemsstaternes kompetence** i forbindelse med sådanne lovovertrædelser.

Med henblik på at fremme effektiv efterforskning og retsforfølgning af cyberbaseret kriminalitet vil Kommissionen endvidere i starten af 2018 fremsætte forslag til at lette grænseoverskridende adgang til **elektronisk bevismateriale**. Kommissionen vil desuden senest til oktober fremlægge sine overvejelser vedrørende betydningen af **kryptering** i strafferetlige efterforskninger.

Baggrund

De seneste tal viser, at de digitale trusler udvikler sig hurtigt, og at cyberkriminalitet i offentlighedens øjne udgør en betydelig trussel: Forekomsten af afpresningssoftwareangreb er steget med 300 %, og de økonomiske tab som følge af cyberkriminalitet steg til det femdobbelte mellem 2013 og 2017 og har ifølge undersøgelser potentiale til at stige med yderligere 400 % inden 2019. 87 % af europæerne ser cyberkriminalitet som en betydelig trussel mod EU's interne sikkerhed.

Den europæiske dagsorden om sikkerhed og midtvejsgennemgangen af strategien for et digitalt indre marked omfatter retningslinjerne for Kommissionens arbejde på dette område og de vigtigste tiltag, der skal øge cybersikkerheden. De foranstaltninger, der foreslås i dag, supplerer de gældende regler og lukker de huller, der er opstået som følge af et trusselsbillede, der har ændret sig siden EU's strategi for cybersikkerhed blev vedtaget i 2013, og opfylder således hovedmålet om at støtte medlemsstaterne i deres bestræbelser på at sikre intern sikkerhed, der er fastsat ved Bratislavaerklæringen og -køreplanen.

Yderligere oplysninger

Spørgsmål og svar - Unionens tilstand 2017 - Cybersikkerhed Kommissionen intensiverer EU's indsats over for cyberangreb

Faktaark om forslag vedrørende cybersikkerhed

Faktaark om EU-agenturet for cybersikkerhed

Faktaark om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter

Dokumenter vedtaget den 13. september

[1] F.eks. er omkostningerne til certificering af intelligente målere i Det Forenede Kongerige og Frankrig ca. 150 000 EUR.

IP/17/3193

Pressehenvendelser:

Natasha BERTAUD (+32 2 296 74 56)
Nathalie VANDYSTADT (+32 2 296 70 83)
Tove ERNST (+32 2 298 67 64)
Maja KOCIJANCIC (+32 2 298 65 70)
Inga HOGLUND (+32 2 295 06 98)

Borgerhenvendelser: Europe Direct på tlf. 00 800 67 89 10 11 eller pr. mail

Attachments

20170919-cybersecurity factsheet non-cash payments-en.pdf
Cybersecurity-EU agency and certification framework.en.pdf
Cybersecurity.en.pdf