Europese Commissie

STAAT VAN DE UNIE 2018

Bouwen aan sterke cyberbeveiliging in Europa

#SOTEU

12 september 2018

"Cyberaanvallen kennen geen grenzen, maar onze responscapaciteit verschilt zeer sterk van land tot land, waardoor lacunes ontstaan en er door kwetsbare punten nog meer aanvallen worden gepleegd. De EU heeft behoefte aan sterkere en doeltreffendere structuren om voor een hoge cyberweerbaarheid te zorgen en om op cyberaanvallen te reageren. Wij willen niet de zwakste schakels zijn ten aanzien van deze wereldwijde dreiging."

Jean-Claude Juncker, digitale top van Tallinn, 29 september 2017

De Europese Commissie en de hoge vertegenwoordiger willen Europa uitrusten met de geschikte instrumenten om het hoofd te bieden aan de voortdurend veranderende cyberdreiging en hebben daarom in 2017 een groot aantal maatregelen voorgesteld om de cyberbeveiliging in de EU te versterken. Deze inspanningen worden nu aangevuld met een voorstel waarmee de EU middelen en deskundigheid op het gebied van onderzoek en innovatie kan bundelen en kan uitgroeien tot een leider op het gebied van cyberbeveiligings- en digitale technologieën van de volgende generatie.

Huidige cyberdreigingen

> 4 000 aanvallen met ransomware per dag in 2016

80 % van de Europese bedrijven heeft het afgelopen jaar met minstens één cyberincident te maken gehad

In alle bedrijfssectoren is het aantal **veiligheidsincidenten met 38 % gestegen** — de grootste stijging van de afgelopen 12 jaar

In sommige lidstaten is cybercriminaliteit goed voor **50 % van alle misdaad**

> 150 landen en > 230 000 systemen in verschillende sectoren en landen werden getroffen door een WannaCry-aanval in mei 2017 en ondervonden een wezenlijke impact op essentiële diensten die verbonden zijn met het internet, bijvoorbeeld ziekenhuizen en ambulancediensten.

Weerbaarheid tegen cyberaanvallen versterken

De Commissie ondersteunt nu al de versterking van het afschrikkingseffect, de weerbaarheid en het reactievermogen van de EU ten opzichte van cyberaanvallen, onder meer door:

De doeltreffende toepassing van de eerste Europese wet inzake cyberbeveiliging (richtlijn inzake de beveiliging van netwerk- en informatiesystemen) te ondersteunen, aan de hand van:

MEER CAPACITEIT

De lidstaten moeten hun capaciteit op het gebied van cyberbeveiliging verbeteren

SAMENWERKING

Intensievere samenwerking op EU-niveau

RISICOPREVENTIE

De actoren in belangrijke sectoren (zoals die van energie, transport en gezondheid) zijn verplicht maatregelen in te voeren om risico's te voorkomen en cyberincidenten aan te pakken

Samen te werken met de lidstaten op het gebied van:

EU-AGENTSCHAP VOOR CYBERBEVEILIGING

Het agentschap van de Europese Unie voor cyberbeveiliging versterken om de lidstaten beter bij te staan

EU-CERTIFICERINGSREGELING

Een EU-brede certificeringsregeling om de cyberveiligheid van producten en diensten te waarborgen

GECOÖRDINEERDE RESPONS

Zorgen voor snelle en gecoördineerde respons op grootschalige cyberaanvallen

Het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) helpt de cyberbeveiligingsautoriteiten van de lidstaten om de EU beter te beschermen tegen cyberaanvallen.

Middelen en deskundigheid op het gebied van cyberbeveiligingstechnologie bundelen

Naast de reeds bestaande initiatieven van de EU op het gebied van cyberbeveiliging stelt de Commissie vandaag voor deze inspanningen aan te vullen met de oprichting van een netwerk van kenniscentra en een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging met het oog op de ontwikkeling en inzet van instrumenten en technologieën die nodig zijn om gelijke tred te houden met de voortdurend veranderende dreigingen.

Het Europees centrum zal samen met de lidstaten de voor cyberbeveiliging uitgetrokken middelen uit hoofde van de volgende langetermijnbegroting van de EU op de meest gerichte manier coördineren. Hierdoor zullen nieuwe Europese cybervermogens tot stand komen.

Europa beschikt al over een schat aan deskundigheid - over de hele EU zijn meer dan **660 kenniscentra voor cyberbeveiliging** verspreid. Om doeltreffend gebruik te maken van hun deskundigheid stelt de Commissie een mechanisme voor om:

De bestaande deskundigheid te bundelen, te delen en beschikbaar te stellen

Producten en oplossingen op het gebied van cyberbeveiliging in de EU te helpen inzetten

Te zorgen voor langdurige strategische samenwerking tussen industrieën, de onderzoeksgemeenschap en overheden

Gezamenlijk te investeren in dure infrastructuur en deze te delen

Europees kenniscentrum:

Zal het gebruik van de voor cyberbeveiliging uitgetrokken middelen uit hoofde van de volgende langetermijnbegroting van de EU voor 2021-2027 coördineren in het kader van de programma's Digitaal Europa en Horizon Europa. Het centrum zal ondersteuning bieden aan het netwerk en de gemeenschap om onderzoek en innovatie op het gebied van **cyberbeveiliging** te stimuleren. Het zal ook **gezamenlijke investeringen** door de EU, de lidstaten en de industrie op poten zetten. Zo zal in het kader van het programma Digitaal Europa **2 miljard EUR** worden geïnvesteerd in de bescherming van de Europese digitale economie, samenleving en democratie door de cyberbeveiligingssector van de EU te stimuleren en geavanceerde apparatuur en infrastructuur voor cyberbeveiliging te financieren.

Netwerk van nationale coördinatiecentra:

Elke lidstaat zal een nationaal coördinatiecentrum aanwijzen om het netwerk te leiden, dat zich zal bezighouden met de ontwikkeling van nieuwe capaciteiten op het gebied van cyberbeveiliging en de opbouw van bredere deskundigheid. Het netwerk zal de meest relevante projecten op het gebied van cyberbeveiliging in de lidstaten helpen selecteren en ondersteunen.

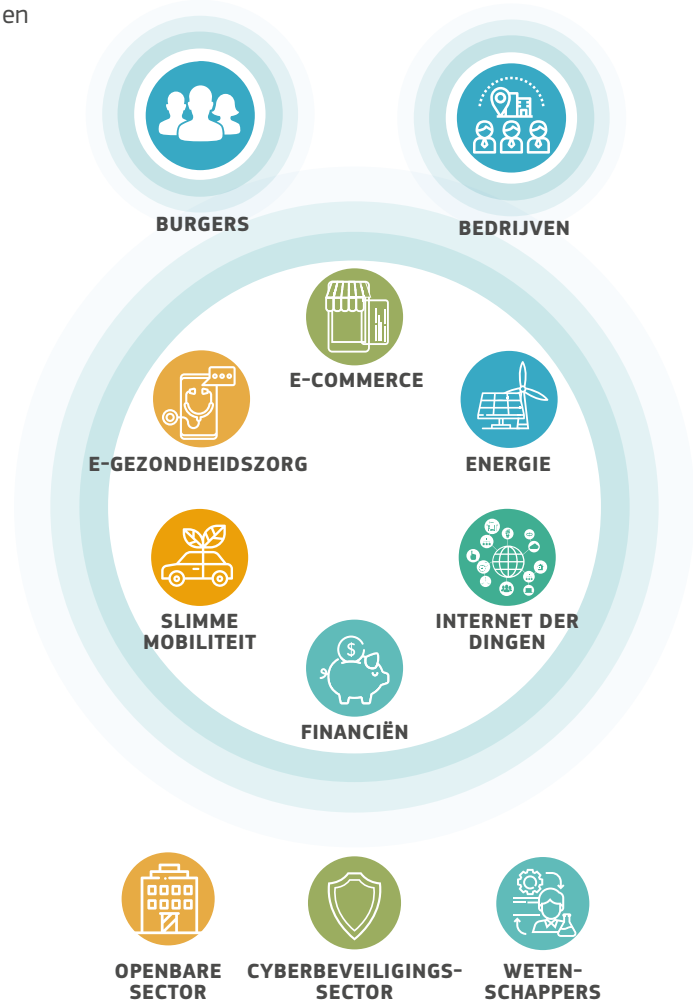
Kennisgemeenschap:

Een grote, open en diverse groep belanghebbenden op het gebied van cyberbeveiliging uit de onderzoeksgemeenschap en de particuliere en openbare sector, waaronder zowel civiele als militaire autoriteiten.

Wat zijn de verwachte verbeteringen?

- betere coördinatie van werkzaamheden;
- toegang tot deskundigheid;
- toegang tot test- en experimenteerfaciliteiten;
- beoordeling van de cyberbeveiliging van producten;
- toegang tot innovatieve producten en oplossingen op het gebied van cyberbeveiliging;
- ondersteuning van de marktintroductie van producten en diensten;
- grotere zichtbaarheid voor potentiële investeerders en zakenpartners;
- kostenbesparing door gezamenlijke investeringen met andere lidstaten;
- de EU zal in staat zijn om haar economie en democratie zelfstandig te beveiligen;
- de EU zal uitgroeien tot een wereldleider op het gebied van cyberbeveiliging.

Wie heeft hier baat bij?



Publicatiebureau

Print ISBN 978-92-79-92473-6 doi:10.2775/748689 NA-04-18-693-NL-C
PDF ISBN 978-92-79-92471-2 doi:10.2775/417531 NA-04-18-693-NL-N