BRAIN-be
Belgian Research Action through Interdisciplinary Networks

BCC

Meten van kost en impact van cybercrime in België

DUUR
1/12/2013 – 28/02/2018

BUDGET
684.731 €

PROJECT BESCHRIJVING

Achtergrond
Terwijl de digitale transitie enorme mogelijkheden biedt voor de Belgische economie en samenleving, onthult deze ook een nieuwe dreiging in de vorm van cybercrime. Dit kan de openbare en nationale veiligheid in gevaar brengen, evenals vervoer, communicatie, e-commerce, financiële, hulp- en andere diensten die afhankelijk zijn van digitale informatie en infrastructuur. Overheden moeten geïnformeerde beslissingen kunnen nemen om internetgebruikers te beschermen tegen de cyberdreiging en economische groei te bevorderen. De exacte impact veroorzaakt door cybercrime is echter nog onbekend. Dit gebrek aan informatie heeft geleid tot een niet geïnformeerde beleidsvoering en een inconsistente beoordeling van het probleem.

Gezien de verstrekkende gevolgen van cybercrime, is het noodzakelijk om bij het nemen van efficiënte maatregelen verschillende overheidssectoren te betrekken en samen te werken op internationaal niveau. Bewust van de nood aan wetenschappelijk onderzoek, bepaalt de overheid in zijn Federaal regeerakkoord van 2011 om de relevante stakeholders te raadplegen in de strijd tegen cybercrime. Eind 2012 werd een Nationale Cyber Security Strategie voor België goedgekeurd waarin wordt gesteld dat te nemen maatregelen gebaseerd moeten zijn op geïnformeerde besluitvorming. Eind 2013 werd beslist tot oprichting van een Belgisch Cyber Veiligheid Centrum (CCSB). Het bestrijden van cybercrime is een grote uitdaging en vereist van beleidsmakers een goede kennis van de impact van deze dreiging. Een multidisciplinair onderzoek naar de kost en impact van cybercrime zal de uitwerking en uitvoering van een efficiënt federaal overheidsbeleid ondersteunen waardoor België een strategische plaats kan innemen op de internationale scene.

Doelstelling
Het project heeft tot doel een objectief, realistisch en recent beeld te geven van cybercrime in België en de evolutie doorheen de tijd. Een kritische evaluatie van internationale onderzoeksrapporten geeft een overzicht van bestaande kennis rond het meten van de kost en impact van cybercrime en de gebruikte indicatoren. Ondersteund door een Opvolgingscomité worden informatiebronnen rond cybercrime in België geïdentificeerd en geanalyseerd en wordt een taxatie gemaakt van ontbrekende bronnen.

Uitgevoerd over vier jaar, zal het onderzoek een beter geïnformeerd en wetenschappelijk onderbouwd beeld geven van de impact van de cyberdreiging, dankzij een land-specifiek model om de kost en impact van cybercrime te beramen. Het zal ook strategische inzichten en richtlijnen geven voor beleidsmakers over hoe de principes opgenomen in de Belgische Nationale Cyber Security Strategie verder kunnen geïmplementeerd worden.

Methodologie
Het werk wordt verdeeld over werkpakketten die in parallel en op gecoördineerde wijze worden uitgevoerd door de onderzoeksgroepen onder begeleiding van het Opvolgingscomité.

In **WP1** wordt in overleg met het Opvolgingscomité beslist over de **reikwijdte** van het model om de kost en impact van cybercrime in België te meten. Relevante publicaties en bronnen worden opgevolgd, evenals hun mogelijke impact op het **model** dat ontwikkeld en geïmplementeerd wordt in **WP2.**

Verticaal
Drie trajecten zijn uitgetekend om het onderwerp te bevatten en de gegevens erover op te volgen: **Burgers (WP3); Industrie (WP4); Overheid (WP5)**. Het onderzoek in deze drie sectoren vormt de verticale pijlers waarop het model wordt gebouwd.

BCC

Horizontaal
Ter ondersteuning van de verticale pijler, wordt een evaluatie gemaakt van de investeringen in **tegenmaatregelen** die reeds genomen werden door burgers, het bedrijfsleven en de overheid in hun strijd **tegen cybercrime** (**WP6**). Dit levert input voor het meten van de kost als gevolg van cybercrime, en draagt bij aan het model met indicatoren om toekomstige kosten te voorspellen.

Burgers
We gaan de bevolking bevragen over hun ervaringen met het internet en cybercrime, en hoe dit hun gedrag op, en ervaring met het internet beïnvloedt. Deze enquête wordt twee keer uitgevoerd om een longitudinaal onderzoek te krijgen, zodat een evolutie kan worden gemeten.

Industrie
Voor de industriële sector worden data over financiële verliezen als gevolg van online fraude in het bankwezen en de kleinhandel gebruikt om correlaties tussen de verliezen en bepaalde risico-indicatoren te zoeken. Het tracht de technische risico-indicatoren van blootstelling aan het internet te identificeren en hiermee het verlies te modeleren.Veranderingen in de gemeten risico-indicatoren zullen worden bijgehouden evenals de invloed die ze hebben op mogelijke verliezen. Na validatie van de gehanteerde indicatoren kan dit model worden geëxtrapoleerd naar de industriesector als geheel. De steun van koepelorganisaties zal worden gezocht voor de dataverzameling binnen verschillende industriële sectoren (enquete) en voor de beoordeling van het model.

Overheid
Een analyse wordt gemaakt van beschikbare gegevens en bronnen met betrekking tot de publieke sector en een bevraging wordt georganiseerd met steun van het Opvolginggscomité en de BelNIS werkgroep, waarin vertegenwoordigers van verschillende federale entiteiten samenwerken om activiteiten met betrekking tot informatiebeveiliging te coördineren.

Verwachte onderzoeksresultaten

- een methodologie en een model met beproefde indicatoren om op te volgen om een overzicht te krijgen van de omvang van de kost en impact van cybercrime in België.
- een overzicht van de kost en impact van cybercrime in België, verkregen door toepassing van het gebruikte model.

CONTACT INFORMATIE

Coördinator

Marie-Christine Janssens - Ann Mennens
Katholieke Universiteit Leuven (KU Leuven)
Interdisciplinary Centre for Law and ICT
m-ch.janssens@law.kuleuven.be
ann.mennens@law.kuleuven.be

Partners

Pieter Verdegem
Universiteit Gent (UGent)
Research Group for Media & ICT
pieter.verdegem@ugent.be

Wouter Joosen - Christophe Huygens
Katholieke Universiteit Leuven (KU Leuven)
IMinds-DistriNet Research Group @ KU Leuven
wouter.joosen@cs.kuleuven.be
christophe.huygens@cs.kuleuven.be

Vincent Rijmen
Katholieke Universiteit Leuven (KU Leuven)
COSIC @ KU Leuven
vincent.rijmen@esat.kuleuven.be

LINKS

www.icri.be
www.b-ccentre.be
www.mict.be
https://distrinet.cs.kuleuven.be
http://www.esat.kuleuven.be/cosic/

belspo

FEDERAAL WETENSCHAPSBELEID
231 Louizalaan • B-1050 Brussel
Tel. +32 (0)2 238 34 11
http://www.belspo.be/brain-be/ • Email : BRAIN-be@belspo.be

BR/132/A4/BCC