CIBG KATERN 37

NAAR EEN GEWESTELIJK **CYBERVEILIGHEIDSPLAN**

Burgers, bedrijven en besturen veilig online

cibg.brussels
IT is for you

bps-bpv
.brussels
Bruxelles Prévention & Sécurité
Brussel Preventie & Veiligheid

INHOUDSTAFEL

HET BRUSSELS HOOFDSTEDELIJK GEWEST BESCHIKT OVER HEEL WAT KRITIEKE INFRASTRUCTUREN DIE EEN DOELWIT VOOR CYBERCRIMINELEN ZIJN

VOORWOORD

Als kind leren we allemaal om naar links en rechts te kijken voordat we de straat oversteken. We analyseren de risico's, passen preventiemethoden toe en leren indien nodig uit onze fouten. Waarom doen we dat dan meestal niet in de cyberspace?

Het nieuws liegt er niet om: burgers, bedrijven, openbare besturen... Niemand ontsnapt aan cyberaanvallen, die zich met de regelmaat van de klok voordoen. Hoewel er niet meteen mensenlevens op het spel staan, loopt de schade van deze aanvallen al snel op tot miljoenen en zelfs miljarden euro's. Om nog maar te zwijgen van de imagoschade: wee wie de cyberteugels heeft laten vieren! Cyberveiligheid is dus net als de strijd tegen terrorisme een kwestie van nationale veiligheid.

Zijn onze informaticasystemen, die vandaag, in dit tijdperk van Smart Cities en gedeelde oplossingen, een centrale rol spelen op de werkvloer, wel voldoende in staat om bedreigingen te herkennen, voorkomen, overwinnen en er indien nodig van te herstellen?

Het Brussels Hoofdstedelijk Gewest beschikt over heel wat van kritieke infrastructuren waar cybercriminelen het op gemunt hebben vanwege zowel de hoge concentratie inwoners, bedrijven en openbare diensten die in contact staan met miljoenen mensen in diverse domeinen zoals financiën, mobiliteit en gezondheid als de aanwezigheid van internationale instellingen. De openbare sector moet dan ook passende, doeltreffende antwoorden ontwikkelen afhankelijk van de relevante noden en bevoegdheden.

Dit katern biedt een antwoord op deze belangrijke kwestie. Het is het resultaat van een gemeenschappelijke denkoefening van het Centrum voor Informatica voor het Brusselse Gewest (CIBG) en Brussel Preventie & Veiligheid (BPV), en bouwt voort op onze reeds uitgebreide samenwerking. In dit katern maken we een stand van zaken op van cyberdreigingen en schuiven we een methodologisch kader naar voren om er een antwoord op te bieden.

We vertrekken hoegenaamd niet van nul. Zowel het CIBG als BPV komen beslagen op het ijs wat de cyberbeveiliging betreft. Kijk maar naar de infrastructuren (meer bepaald het Gewestelijk Data Center en het IRISnet-netwerk) en IT-beveiligingsdiensten van het CIBG, de conformering aan de nieuwe Algemene Verordening Gegevensbescherming (algemeen bekend onder de Engelse afkorting 'GDPR') en de beveiligingsoplossingen voor klanten. BPV heeft op zijn beurt een van de thema's van zijn globaal veiligheids- en preventieplan dat op 2 februari 2017 werd goedgekeurd door de Regering van het Brussels Hoofdstedelijk Gewest gewijd aan cyberveiligheid. Bovendien wordt er momenteel gewerkt aan samenwerkingsverbanden met spelers uit de beveiligings- en onderwijssector – met name binnen de Gewestelijke school voor veiligheidsberoepen – om de cyberveiligheid in het Brussels Hoofdstedelijk Gewest op de kaart te zetten. De vruchten van deze ontwikkelingen mogen in geen geval verloren gaan.

Daarom wordt het katern afgesloten met een lijst aanbevelingen als eventuele kapstok voor het gewestelijk cyberveiligheidsplan dat nodig is om alle Brusselaars in hun gebruik van digitale diensten en hulpbronnen hun recht op veiligheid te kunnen laten gelden. De invoering hangt niet uitsluitend af van het CIBG en BPV: al wie in ons Gewest met veiligheid bezig is, moet hierbij betrokken worden.

Hervé Feuillien
Directeur-Generaal
CIBG

Robert Herzeele
Adjunct-Directeur-Generaal
CIBG

Jamil Araoud
Directeur-Generaal
BPV

INLEIDING

Het Brussels Hoofdstedelijk Gewest ziet in digitalisering kansen voor de openbare diensten om hun aanbod te verbeteren en zich verder te ontwikkelen tot Smart City-pioniers. Een efficiënte, beveiligde digitale omgeving versterkt bovendien de capaciteiten van privébedrijven: een producten- en dienstenaanbod dat afgestemd is op een wereld die voortdurend evolueert, maakt bedrijven competitiever. Ook de academische sector en verenigingen baten bij (en hebben nood aan) een beveiligde digitale omgeving.

De kosten en risico's die bij digitalisering komen kijken, zijn voor al deze spelers vaak hinderpalen. Wat het prijskaartje makkelijk de hoogte in jaagt, zijn de risico's van cyberspace en de bijbehorende bescherming, die ondertussen onontbeerlijk is geworden.

De toename van het aantal bedreigingen en kwetsbare punten als gevolg van groeiende complexiteit, is een uitdaging waaraan alle spelers in dit economische domein – dat ondertussen niet meer weg te denken is - het hoofd moeten bieden.

Op 20 november 2017 raadde de Raad Algemene Zaken van de Europese Unie aan om de cyberveiligheid en cyberveerkracht in heel Europa te verhogen. We zijn van mening dat het Brussels Hoofdstedelijk Gewest de nodige aandacht aan dit onderwerp moet besteden en een gewestelijk cyberveiligheidsplan moet opstellen.

Het Centrum voor Informatica voor het Brusselse Gewest (CIBG) bevindt zich als vertrouwenspersoon van de gewestelijke, gemeentelijke en communautaire openbare instellingen voor informatica in een bevoorrechte positie om het gewest te helpen cyberspacerisico's in kaart te brengen en zich ertegen te beschermen. Het ligt voor de hand dat het CIBG de partner bij uitstek is voor het dirigeren en uitvoeren van bewustmakings- en corrigerende maatregelen. Het CIBG is de ideale leverancier van basisdiensten en voorziet alle betrokkenen van de nodige basisbescherming.

Daarnaast buigt Brussel Preventie & Veiligheid (BPV) zich in het kader van de uitvoering van het globale veiligheids- en preventieplan (GVPP) en met name de thema's 'aantasting van de menselijke integriteit', 'radicalisering', 'cybercriminaliteit' en 'crisisbeheer en veerkracht' over cybercriminaliteit en de reactie op ernstige digitale incidenten met een grote reële impact.

Het Brussels Hoofdstedelijk Gewest zet al lang de toon op het vlak van automatisering en nieuwe technologieën. Het is dan ook niet meer dan normaal dat de verantwoordelijken van het gewest niet bij de pakken blijven zitten, maar een passend, vooruitziend en flexibel gewestelijk cyberveiligheidsplan voorstellen.

Op basis van bestaande gewestelijke, nationale en Europese initiatieven zal het de prioriteiten van dat plan optimaal kunnen afstemmen op de belangrijkste doelstellingen en risico's.

Het plan moet de huidige omgeving zo goed mogelijk beschrijven, de risico's en bedreigingen evalueren en prioritaire maatregelen voorstellen voor de belangrijkste actoren binnen het Brussels Gewest: openbare diensten, privébedrijven, onderwijsinstellingen en vooral de burgers zelf. De methoden in dit plan steunen op erkende en recente referentiekaders en beproefde praktijken.

Het plan is ambitieus en om het meeste te halen uit digitalisering en de bijbehorende voordelen voor de concurrentiepositie van de actoren in ons gewest, zal het doelpubliek de nodige voorzichtigheid en doorzettingsvermogen aan de dag moeten leggen.

Professor Georges Ataya
Academisch directeur van de informatie- en cyberveiligheidsopleidingen
van de Solvay Brussels School of Economics and Management

© John Stapels

CYBERVEILIGHEID IS NET ALS DE STRIJD TEGEN TERRORISME EEN KWESTIE VAN NATIONALE VEILIGHEID.

1.

2017 was een jaar waarin cyber(on)veiligheid niet uit het nieuws weg te slaan was. Twee voorbeelden daarvan zijn WannaCry en NotPetya, die op luttele weken van elkaar uitbraken in mei en juni 2017. Plots werd de aandacht van het grote publiek gevestigd op niet alleen cyberdreiging, maar ook – en vooral – op de kwetsbaarheid van onze informaticasystemen.

1. VAN CYBERCRIMINALITEIT TOT -CONFLICTEN

Niets of niemand blijft gespaard van cyberdreiging. Niet alleen individuele gebruikers – die eraan ten prooi vallen door bepaalde websites te bezoeken, achteloos te handelen (bijv. een bijlage bij een dubieuze e-mail openen) of hun pc's of smartphones onvoldoende te beveiligen – worden tegenwoordig het slachtoffer van cyberaanvallen. Wie slechte bedoelingen heeft, heeft niet meer dan enkele uren nodig om een multinational of een administratie lam te leggen waar honderden miljoenen gebruikers op rekenen. Om nog maar te zwijgen van aanvallen die de stabiliteit van een land zelf viseren.

We worden geconfronteerd met een onhoudbare toename van gegevenslekken en kwetsbare punten in informaticasystemen. In IBM's rapport over 2016 schat de beveiligingsafdeling van het bedrijf het aantal gelekte/beschadigde gegevens in de loop van het jaar op meer dan 4 miljard, een stijging van 566% tegenover 2015[1]. Nog onrustwekkender is dat IBM een verschuiving in de georganiseerde cybercriminaliteit merkt: hoewel ook particulieren gevaar blijven lopen, zijn professionele gebruikers, de zogenaamde 'corporate accounts' tegenwoordig de favoriete prooi.

> WIE SLECHTE BEDOELINGEN HEEFT, HEEFT NIET MEER DAN ENKELE UREN NODIG OM EEN MULTINATIONAL OF EEN ADMINISTRATIE LAM TE LEGGEN

Die verschuiving onthult het vaakst geciteerde motief voor cybercriminaliteit: geld. Bedrijven en instellingen aanvallen brengt meer op omdat ze doorgaans beter bij kas zijn dan natuurlijke personen. In het IBM-rapport stelt men het als volgt: "*Georganiseerde bendes zijn geneigd om bedrijven te viseren omdat er daar in één keer heel wat meer geld te rapen valt dan bij consumentenrekeningen. In de arena van cybercriminaliteit zijn bendes het type gladiatoren die de nodige wapens hebben om grotere hoeveelheden geld te stelen.*"

Cyberaanvallen worden niet alleen gelanceerd om rijk te worden. Ze kunnen ook gebruikt worden om machtsverhoudingen tussen landen, met name op politiek en militair vlak, te beïnvloeden. "*Cyberaanvallen kunnen gevaarlijker zijn voor de stabiliteit van democratieën en economieën dan geweren en tanks*", zei Jean-Claude Juncker, voorzitter van de Europese Commissie, in zijn State of the Union in september 2017. De grens tussen cybercriminaliteit en -conflicten is soms vaag. Zo leidde de WannaCry-aanval tot een krasse, weinig subtiele beschuldiging van Microsoft aan het adres van de Amerikaanse National Security Agency (NSA). WannaCry werd mogelijk gemaakt via een hackingtool die profiteerde van een beveiligingslacune in besturingssystemen zoals Windows 7 en XP. De tool, een geducht

1 Onderzoek bij een steekproef van meer dan 8.000 IBM-klanten in 100 landen. Bron: IBM X-Force Threat Intelligence Index, online (geraadpleegd op 22/12/2017). Zie https://www.ibm.com/security/data-breach/threat-intelligence-index.html.

cyberwapen, was door de NSA in het grootste geheim, ook voor Microsoft, ontwikkeld, maar werd daarna van de inlichtingendienst gestolen. Naar aanleiding van het misbruik van die tool voor WannaCry publiceerde Microsoft een persbericht waarin het hoofd van juridische zaken het volgende zegt: "*Deze zoveelste aanval illustreert perfect waarom de ketting vol kwetsbare schakels bij overheden zo'n groot probleem is. Dit type aanvallen is een van de trends van 2017. [...] En deze nieuwste aanval symboliseert een geheel onbedoelde maar verontrustende wisselwerking tussen de twee belangrijkste actoren in cyberdreiging vandaag – de staat en de georganiseerde misdaad.*" [2]

Staten gebruiken ter verdediging niet alleen dezelfde tools als cybercriminelen en -terroristen, maar zijn soms amper van hen te onderscheiden. Cyberspace is het nieuwe werkterrein geworden van inlichtingendiensten. Het vermogen van staten om via cyberaanvallen destabilisering te provoceren, is reëel. De laatste presidentsverkiezingen in de Verenigde Staten en Frankrijk illustreren dit perfect. In beide gevallen heeft het lekken van gevoelige computergegevens, toegeschreven aan een vreemde mogendheid, de presidentiële campagnes zo in gevaar gebracht dat veel analisten er de nederlaag van Hillary Clinton aan weten. Het vermogen om de publieke opinie via sociale media te manipuleren is nog zo'n wereldwijd risico dat door het Wereld Economisch Forum werd aangeduid op basis van de vaststelling dat 63% van sociale-mediagebruikers daar ook zijn nieuws haalt.

2. GLOBALISERING VAN RISICO'S DOOR NETWERKEN

Voor een cyberaanval heeft men toegang nodig tot een bepaalde computer of een heel informaticasysteem. Die toegang kan worden verschaft via een fysieke drager. Zo zat Brain, een van de eerste en gevaarlijkste virussen, verborgen op diskettes. Maar de mogelijkheden om cyberaanvallen te verspreiden hebben zich pas echt vermenigvuldigd sinds de ontwikkeling van informaticanetwerken. In 1972 al ontdekte een onderzoeker een manier om de toestellen te besmetten die gekoppeld waren aan ARPANET, een netwerk van het Amerikaanse leger en voorloper van het internet. Tijdens de opmars van het netwerk der netwerken groeide ook de cyberdreiging razendsnel: van omstreeks 1990 tot 2010 is het aantal malwaresoftware gestegen van zo'n 1000 entiteiten naar meer dan 200 miljoen. In de jaren 2000 kwamen daar de eerste aanvallen op mobiele terminals bij.

Zoals het Wereld Economisch Forum (WEF) stelt, is onze toenemende afhankelijkheid van het internet en informatie- en communicatietechnologie (ICT) uitgegroeid tot een van de grootste wereldwijde risicobronnen, waaronder cybercriminaliteitrisico's. In het besluit van de editie van 2017 van The Global Risks Report schrijft het WEF: "*De grotere afhankelijkheid tussen infrastructuurnetwerken werkt een bredere scope voor systematische mislukkingen in de hand – of die nu het gevolg zijn van cyberaanvallen, softwarefouten, natuurrampen of iets anders – die zich uitbreiden door netwerken heen en de samenleving op onverwachte manieren beïnvloeden.*"

2 SMITH, Brad. The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Microsoft On the Issues, Microsoft, online (geraadpleegd op 22/12/2017). Zie https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack.

Elke nieuwe aanval leidt tot deze twee vragen: wie is de volgende en op welke schaal? Een gezamenlijke studie van consultancybureau KPMG en rekruteringsbedrijf Harvey Nash [3] geeft duidelijk weer hoe kwetsbaar informaticasystemen zijn. Volgens het onderzoek, waarvoor 4000 CIO's (Chief Information Officers) in 86 landen werden ondervraagd:

- heeft een derde van de CIO's de afgelopen twee jaar te maken gehad met een lacune in de informaticabeveiliging; bij grote bedrijven is dat één op twee;
- bevestigt maar een vijfde van de CIO's (21%) dat zijn organisatie een cyberaanval het hoofd kan bieden;
- noemt bijna één op twee CIO's (47%) aanvallen van binnenuit een van zijn grootste kopzorgen in 2017.

Het Belgische luik van het onderzoek van KPMG/Harvey Nash laat zien dat de situatie in ons land nog onrustwekkender is: "*Meer dan 42% van de bedrijven in België zijn de afgelopen 2 jaar het slachtoffer geworden van grote cyberaanvallen. Bovendien geven Belgische bedrijven aan dat ze zich minder zeker en onvoldoende voorbereid voelen om huidige en toekomstige aanvallen het hoofd te bieden in vergelijking met het wereldwijde gemiddelde.* [4]"

De acute aard van de dreiging wordt ook aangehaald door het EU-agentschap voor de beveiliging van netwerken en informatie, het European Network and Information Security Agency (ENISA [5]). Volgens ENISA's jaarlijkse lijst met de 15 grootste cyberdreigingen van 2017 wordt er maar 1 dreiging kleiner, terwijl er 11 groter worden. Dat is een negatieve evolutie in vergelijking met 2016, toen er maar 9 dreigingen groter waren geworden.

ENISA laat verder weten dat "de complexiteit van de aanvallen en de precisie van kwaadaardige handelingen in de cyberspace blijven stijgen". Het Europese agentschap bepaalt op basis van haar observaties van de cyberdreiging in 2017 de volgende zes opmerkelijke feiten:

- Hackers en cybercriminelen van alle dreigingstypes wissen hun sporen beter uit.
- De kwaadwillige infrastructuur blijft evolueren met flexibele functies afhankelijk van het doel: anonimisering, encryptie, ontwijkingsmogelijkheden (wat het detecteren van indringers in de war stuurt).
- Geld verdienen met cybercriminaliteit wordt het belangrijkste doel van hackers en vooral cybercriminalen, die hun voordeel halen uit de anonimiteit van cybergeld.
- Door de staat gesteunde actoren behoren tot de belangrijkste aanvallers in de cyberspace en staan bovenaan de prioriteitenlijst van de commerciële en overheidsactoren die zich ertegen moeten beschermen.
- De cyberoorlog zet de cyberspace op zijn kop en zorgt zo voor kopzorgen bij infrastructuurbeheerders, vooral in domeinen die lijden onder bepaalde types cybercrises.
- Kennen en kunnen blijven de grootste werkpunten van organisaties. De opleidingen en cursussen met aandacht voor het bestrijden van cyberdreigingen zijn zeer schaars.

3 KPMG Belgium. Harvey Nash/KPMG International CIO Survey 2017. Press releases, KPMG Belgium, 18 augustus 2017, online (geraadpleegd op 22/12/2017). Zie https://home.kpmg.com/be/en/home/media/press-releases/2017/08/harvey-nash-kpmg-international-cio-survey-2017.html.

4 KPMG Belgium. Harvey Nash/KPMG International CIO Survey 2017. Press releases, KPMG Belgium, 18 augustus 2017, online (geraadpleegd op 22/12/2017). Zie https://home.kpmg.com/be/en/home/media/press-releases/2017/08/harvey-nash-kpmg-international-cio-survey-2017.html

5 Lees meer over de rol en de werking van het ENISA op pagina 32 in rubriek 3.2. "Belangrijkste spelers in cyberveiligheid"

DE 15 GROOTSTE CYBERDREIGINGEN, OPGETEKEND IN 2017*

Plaats	Dreiging**	Trend	Evolutie 2016 - 2017***
1	Malware	→	=
2	Aanvallen afkomstig van het web	↑	=
3	Aanvallen op webapplicaties	↑	=
4	Phishing	↑	+2
5	Spam	↑	+2
6	Denial-of-service	↑	-2
7	Gijzelsoftware	↑	+1
8	Botnets	↑	-3
9	Interne dreiging (kwaadwillig of onbedoeld)	→	=
10	Beschadiging/diefstal/fysiek verlies	→	=
11	Gegevensinbreuken	↑	+1
12	Identiteitsdiefstal	↑	+1
13	Informatie-/gegevenslekken	↑	+1
14	Exploitkits	↓	-3
15	Cyberspionage	↑	=

*Bron: ENISA, Threat Landscape 2017 report: cyber-threats becoming top priority, januari 2018.[6]
**Zie tabel Hulpmiddelen en strategieën van cybercriminelen op pagina 16 en 17 voor een definitie van de dreigingen.
***Aantal plaatsen dat de dreiging gestegen of gedaald is ten opzichte van het voorgaande jaar.

3. BASISDIENSTEN ALS DOELWIT

"*Het zou mij niet verbazen als men binnen vijf jaar probeert het internet te gebruiken om aanslagen te plegen, bijvoorbeeld om in te breken in de Scada (n.v.d.r.: Supervisory Control and Data Acquisition) of het beheerssysteem van kerncentrales, stuwdammen of het spoor- of luchtverkeer*", aldus Gilles de Kerchove, EU-coördinator van de strijd tegen terrorisme, kort na de aanslagen van 22 maart 2016 [7].

De openbare diensten en met name **nutsbedrijven** blijven uiteraard niet gespaard. En er zijn voorbeelden genoeg. Het bekendste deed zich voor in Oekraïne, waar eind december 2016 zo'n 700.000 huishoudens zonder elektriciteit kwamen te zitten als gevolg van het eerste algemeen erkende geval van geslaagde cybersabotage van het elektriciteitsnet van een heel land [8]. Enkele maanden later, in juni 2017, werd Oekraïne opnieuw zwaar getroffen, deze keer door de NotPetya-aanval, die het metronetwerk van Kiev en de controle over de kerncentrale in Tsjernobyl viseerde.

6 Het volledige rapport (in het Engels) kan worden gedownload op www.enisa.europa.eu/news/enisa-news/enisareport-the-2017-cyber-threat-landscape.
7 de KERCHOVE, Gilles. Attentats: D'ici 5 ans, ils pourraient prendre le contrôle d'une centrale nucléaire. (Aanslagen: binnen de vijf jaar nemen ze misschien de controle van een kerncentrale over.) La Libre Belgique, IPM, 26/03/2016, online (geraadpleegd op 22/12/2017). Zie http://www.lalibre.be/actu/belgique/attentats-d-ici-5-ans-ils-pourraient-prendre-le-controle-d-une-centrale-nucleaire-56f58f4d35708ea2d3e8e878
8 COLLINS, Katie. Ukraine blackout is a cyberattack milestone. CNET – Security, CNET, CBS Interactive, 05/01/2016, online (geraadpleegd op 22/12/2017). Zie https://www.cnet.com/news/cyberattack-causes-widespread-power-blackout-in-ukraine/

De **gezondheidszorgsector en vooral ziekenhuizen** zijn ook doelwitten van cyberaanvallen. Zo stuurde WannaCry in mei 2017 de diensten van de Britse National Health Service (NHS) in de war. In februari 2016 legde de cyberaanval op het Hollywood Presbyterian Medical Center in Los Angeles de algemene kwetsbaarheid van de sector bloot: het werk moest een tiental dagen lang noodgedwongen neergelegd worden. Daarbij gingen er niet minder dan 900 patiëntendossiers verloren. Uiteindelijk werd er zo'n 15.000 USD losgeld betaald om het informaticasysteem van het ziekenhuis opnieuw te laten werken. Dit is geen uitzondering: Amerikaanse media maakten toen bekend dat vier andere ziekenhuizen al zulke aanvallen hadden ondergaan. Volgens Symantec, leverancier van informatiebeveiligingsdiensten, zijn medische gegevens de heilige graal voor cyberhackers. "*Medische fiches bevatten bijna alle gegevens waar datahackers op azen, wat ze het perfecte doelwit maakt voor eenmalige, allesomvattende diefstal*," aldus Symantec [9]. Het risico wordt verder vergroot door de aard van de sector: versnippering van vaak kleine sites, een gebrek aan goede cyberveiligheidspraktijken bij het personeel, geringe investeringen in informaticabeveiliging en een sterke toename van met het internet verbonden materiaal dat cybercriminelen extra toegangswegen biedt door gebrekkige beveiliging.

De heuse explosie van verbonden voorwerpen (Internet of Things) in aantal en veelzijdigheid ligt aan de basis van toenemende ongerustheid bij informaticabeveiligingsspecialisten. Die voorwerpen zijn immers net zoals de traditionele terminals (pc, smartphone) waar ze op kunnen worden aangesloten vatbaar voor cyberdreigingen doordat ze verbonden zijn met een netwerk. Die kwetsbaarheid wordt versterkt doordat de beveiliging van geconnecteerde voorwerpen vaak niet opgewassen is tegen de aanvallen die ze zelf mee kunnen verspreiden. Naast het hierboven vernoemde medische materiaal zijn ook voorwerpen als een op afstand bedienbare thermostaat kwetsbaar: dit gadget, een zogezegde domoticatopper, kan de smartphone van de gebruiker blootstellen aan hackers. Ook de beveiligingsuitrusting zelf ontkomt er niet aan: in mei 2017 werd een leverancier van informaticamateriaal door de Federal Trade Commission (FTC) voor de rechter gesleept wegens gebrekkige beveiliging van met het internet verbonden bewakingscamera's. Nu na verbonden ook zelfrijdende wagens het stadium van prototype verlaten, worden ze vast het volgende doelwit van cyberaanvallen. De gebrekkige beveiliging van verbonden voorwerpen is ook een kopzorg voor de beheerders van Smart Cities, die meer dan ooit gebruikmaken van sensoren die zijn aangesloten op het netwerk van noodzakelijke diensten zoals nutsvoorzieningen (energie, water...), verkeer, veiligheid...

DE GEBREKKIGE BEVEILIGING VAN VERBONDEN VOORWERPEN IS OOK EEN KOPZORG VOOR DE BEHEERDERS VAN SMART CITIES

9 Symantec. Cybersecurity in Healthcare: Why It's Not Enough, Why It Can't Wait. (Grafische voorstelling). Symantec - Healthcare Symantec, Symantec, online (geraadpleegd op 22/12/2017). Zie https://www.symantec.com/content/dam/symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf.

HULPMIDDELEN EN STRATEGIEËN VAN CYBERCRIMINELEN

Advanced persistent threat (APT)	Backdoor (achterdeurtje)	Botnet
Aanval via meerdere technieken (phishing, malware, exploitkit...) over een langere periode om bepaalde gegevens/processen te beschadigen/aan te tasten	Toegang tot een bepaald softwarepakket (waar de gebruiker geen weet van heeft) met een gerechtvaardigd doel (bijv. updates op afstand zoals gepland door de softwareontwikkelaar) maar eventueel ook met kwaad opzet te gebruiken (om controle te krijgen over de softwaregegevens of in het algemeen de computer of het netwerk waar het deel van uitmaakt)	Computernetwerk waar men zonder medeweten van de gebruiker via code op afstand de controle over kan nemen (overgenomen computers worden ook 'zombies' genoemd) om ze in te zetten voor Distributed Denial-of-Service-aanvallen
Distributed Denial-of-Service	**Exploitkit**	**Gijzelsoftware (ransomware)**
Aanval waarbij een groot aantal toestellen (meestal binnen een botnet) wordt ingezet om massaal verzoeken te verzenden	Pakket van gegevens of stukjes uitvoerbare code waarmee op zoek wordt gegaan naar beveiligingslacunes in de software en het besturingssysteem van een toestel om het te besmetten, gegevens te stelen, enz.	Schadelijke software die per e-mail of via internet wordt ontvangen en die een computer of netwerk blokkeert door bestanden of de hele computer te vergrendelen, waarna losgeld wordt geëist van de gebruiker in ruil voor de sleutel van de code
Rootkit	**Spam**	**Spear-phishing**
Geheel van informaticatools waarmee stiekem op het diepste niveau (root = administrator) de controle over een computer wordt overgenomen en zo de hoogste gebruikersrechten verworven worden	Spam is algemeen bekend als ongewenste berichten waarmee inboxen vaak worden overspoeld; de term verwijst meer bepaald naar dragers die via schadelijke bijlagen informaticasystemen besmetten. In december 2016 bevatte volgens IBM bijna 50% van de spam malware in de vorm van bijlagen, waarvan 85% gijzelsoftware [9]	Variant op phishing die erin bestaat een beperkt aantal gebruikers (vaak maar één) een bericht te sturen dat op basis van social engineering (verzamelen van zo veel mogelijk informatie over het doelwit via onder meer publieke bronnen en sociale media) volledig gepersonaliseerd is
Wiper	**Zero day**	
Schadelijke software die de gegevens van de computer wist zonder dat ze kunnen worden gerecupereerd	Een voor de softwareuitgever onbekende fout die de maker van de fout een groot voordeel biedt omdat er nog geen oplossing voor is	

10 IBM X-Force Threat Intelligence Index. Zie hoger.

	Darknet	**Denial-of-Service**
	Het Darknet wordt vaak omschreven als 'het verborgen internet' en steunt op georganiseerde anonimiteit van zowel de websites als de gebruikers. Het is dan ook een toevluchtsoord voor dissidenten en organisaties, maar wordt ook gebruikt om illegaal diensten en producten te verspreiden, waaronder software en materiële en/of menselijke middelen die worden ingezet voor cyberaanvallen	Het massaal verzenden van verzoeken om een netwerk of dienst zo te verzadigen dat de dienstverlening geheel of gedeeltelijk wordt verhinderd
	Malware	**Phishing**
	Algemene benaming voor schadelijke software die zonder medeweten van de gebruiker toegang verleent tot een toestel, zoals spyware, virussen, Trojaanse paarden, wormen, rootkits, gijzelsoftware, browserkapers, enz.	Het verzending van een algemene boodschap aan een groot aantal geadresseerden, waarbij men zich voordoet als een vertrouwde bron (bank, dienstverlener, openbaar bestuur...) om de slachtoffers bepaalde gegevens te ontfutselen (gebruikersnaam en wachtwoord, pincode...)
	Trojaans paard	**Water holing**
	Techniek die erin bestaat om software die de gebruiker zelf downloadt te gebruiken als spreekwoordelijk Trojaans paard waar men andere, ongevraagde en meestal schadelijke software in verstopt	De naam van dit type aanval verwijst naar de werkwijze van een roofdier dat zijn slachtoffer op een bepaalde plek of een bepaald moment (de watering hole of drinkplaats) opwacht. De hacker profiteert van een beveiligingslacune die hij op het spoor komt via bepaalde gewoonten van het slachtoffer om zich toegang te verschaffen tot een zwaar beveiligd systeem. Zo werden begin 2017 verschillende Poolse banken met malware besmet naar aanleiding van hun herhaalde bezoeken aan de website van de nationale markttoezichthouder

2.

Ons ontwerp voor een cyberveiligheidsplan voor het Brussels Hoofdstedelijk Gewest is gebouwd op stevige funderingen die voortvloeien uit een benchmarking van de benaderingen in andere landen die steunen op beproefde methodologieën.

1. BENCHMARKING VAN EEN OVERHEIDSBELEID OP HET GEBIED VAN CYBERBEVEILIGING

Als we de doelstellingen en methoden willen bepalen die als inspiratie kunnen dienen voor de cyberveiligheidsstrategie van het Brussels Hoofdstedelijk Gewest, moet er een overzicht opgesteld worden met een overheidsbeleid inzake cyberveiligheid.

In het kader hiervan onderzoekt deze benchmarking de strategieën van de buurlanden van België en andere regio's binnen een federale structuur, wat essentieel is bij het opstellen van een gewestelijke strategie.

1.1. Omvang van de benchmarking

Op federaal niveau

Alle lidstaten van de Europese Unie hebben een cyberveiligheidsstrategie opgesteld en organen en methoden in het leven geroepen om die uit te voeren. Sommige landen vallen op door de maturiteit van hun aanpak in die zin dat hun plannen al geëvolueerd zijn. Dat is het geval voor twee buurlanden van België: Nederland en Luxemburg. Verder hebben we de situatie in Estland onderzocht, een land dat al in 2007 werd getroffen door een algemene cyberaanval [1] en waar tegenwoordig het Cooperative Cyber Defence Centre of Excellence (CCDCOE) [2] van de NAVO gevestigd is.

Op regionaal niveau binnen federale staten

Er zijn niet meteen voorbeelden van cyberveiligheidsstrategieën in buurregio's van België te vinden. Zo hebben de twee Duitse bondslanden die aan ons land grenzen, Nordrhein-Westfalen en Rheinland-Pfalz, nog geen strategie op dat vlak. De Franse regio's beschikken noch over de bevoegdheid noch over de capaciteiten om zo'n strategie in te voeren.

We moesten dan ook verder gaan kijken om de strategie te onderzoeken van een regio binnen een federale staat. We zochten en vonden zo'n strategie in Quebec. De Canadese provincie beschikt over een informatieveiligheidsstrategie met een luik rond cyberveiligheid dat in het kader van de benchmarking werd geanalyseerd.

1.2. Krachtlijnen van een cyberveiligheidsstrategie

Uit de vergelijking van de strategieën blijken drie gemeenschappelijke doelen:

- het garanderen van geschikte beveiliging van openbare besturen en kritieke infrastructuren tegen cyberdreigingen
- het verhogen van het vertrouwen van de burger in cyberspace door de strijd aan te binden met de cybercriminaliteit
- het aanscherpen van de eigen competenties op het vlak van cyberveiligheid

1 De gebeurtenissen in Estland in 2007 worden vaak geciteerd als het eerste voorbeeld in de geschiedenis van het internet van een georganiseerde aanval door een land op de netwerken van een ander land.
2 Kijk voor meer informatie over dit uitmuntendheidscentrum voor samenwerking inzake cyberverdediging op de website https://ccdcoe.org/.

De strategieën die we in onze benchmarking onderzocht hebben, steunen trouwens op drie vergelijkbare benaderingen:

- het aanscherpen van de expertise en kennis van openbare besturen, bedrijven en burgers op het vlak van cyberveiligheid
- de ontwikkeling van internationale (en interregionale) samenwerking en coördinatie
- de centralisering van maatregelen en toezicht inzake cyberveiligheid.

Bovendien volgen de concrete maatregelen voor cyberveiligheid in de onderzochte gevallen hetzelfde methodologische kader: het Cybersecurity Framework (CSF), dat is opgesteld door het National Institute of Standards and Technology (NIST) in de VS ter bescherming van de kritieke infrastructuren van een land (zie pagina's 27 en 41).

2. CYBERVEILIGHEID: DEFINITIE?

Waartegen moeten we ons verdedigen en wat zijn onze doelen en middelen wanneer we het hebben over cyberveiligheid? Er zijn hier tal van actoren bij betrokken met elk hun eigen definitie van cyberveiligheid. Onze visie voor het Brussels Hoofdstedelijk Gewest is geïnspireerd door de onderstaande bronnen.

2.1. Op internationaal niveau

In 2010 keurde de **Internationale Telecommunicatie-Unie (ITU)** de onderstaande definitie van cyberveiligheid goed: "*Het geheel van hulpmiddelen, beleidslijnen, beveiligingsconcepten, veiligheidsmechanismen, richtlijnen, risicobeheermethoden, maatregelen, opleidingen, beste praktijken, waarborgen en technologieën die kunnen worden ingezet om de cyberomgeving en de middelen van organisaties en gebruikers te beschermen. De middelen van organisaties en gebruikers omvatten geconnecteerde informaticahulpmiddelen, personeel, infrastructuur, applicaties, diensten, telecommunicatiesystemen en alle informatie die wordt doorgezonden en/of opgeslagen in de cyberomgeving. Cyberveiligheid streeft ernaar de beveiligingskenmerken van de middelen van organisaties en gebruikers te verzorgen en te handhaven om het hoofd te bieden aan de risico's die afbreuk doen aan de veiligheid in de cyberomgeving. De algemene doelstellingen op het vlak van beveiliging zijn: beschikbaarheid, integriteit (die de authenticiteit en de onweerlegbaarheid kan omvatten), vertrouwelijkheid.*" [3]

De **Europese Unie** definieert het begrip in haar Strategie inzake cyberveiligheid [4], die werd gepresenteerd in februari 2013 en bijgewerkt in september 2017. Volgens de Europese Unie is "*cyberveiligheid erop gericht de beschikbaarheid en integriteit van netwerken en infrastructuur in stand te houden, alsmede de vertrouwelijkheid van de informatie die zich daarin bevindt.*" Om dit te bereiken wordt in de strategie de nadruk gelegd op "*de waarborgen en acties [implementeren] die kunnen worden toegepast om de cyberspace op zowel burgerlijk als militair gebied te beschermen tegen dreigingen die gepaard gaan met of schade kunnen aanrichten aan onderling afhankelijke netwerken en de informatie-infrastructuur.*" Bovendien wijst de Europese Commissie erop dat het handhaven van

3 Internationale Telecommunicatie-unie. Les décisions phares de Guadalajara : cybersécurité. (Belangrijkste beslissingen in Guadalajara: cyberbeveiliging.) Onlineverslag van de Conferentie van gevolmachtigden van de ITU in 2010 in Guadalajara, Nouvelles de l'UIT, ITU, november 2010, online (geraadpleegd op 16/02/2018). Zie http://www.itu.int/net/itunews/issues/2010/09/20-fr.aspx.

4 Europese Commissie, hoge vertegenwoordiger van de Europese Unie voor buitenlandse zaken en veiligheidsbeleid. Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace. 7/2/2013, Brussel, online (geraadpleegd op 30/05/2018). Zie https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52013JC0001.

de cyberveiligheid ook essentieel is in het kader van de grondrechten van de Europese burgers, door te stellen dat "*voor cyberbeveiliging [...] een essentiële rol [is] weggelegd bij de bescherming van de persoonlijke levenssfeer en de persoonsgegevens voor personen in overeenstemming met de artikelen 7 en 8 van het Handvest van de grondrechten van de EU.*" [5]

Ter gelegenheid van de 70e verjaardag van de **Internationale Organisatie voor Standaardisatie (ISO)** in februari 2017 noemde de toenmalige voorzitter cyberveiligheid een van de wereldwijde uitdagingen waaraan in de toekomst het hoofd moet worden geboden, naast klimaatverandering en waterschaarste [6]. De ISO plaatst cyberveiligheid in de normenfamilie ISO/CEI 2700x, die de organisatie beschrijft als de gereedschapskist van beveiligingsnormen die organisaties moeten beschermen tegen cyberaanvallen.

In die gereedschapskist vinden we onder meer:

- de norm ISO/CEI 27001:2013 die betrekking heeft op de implementatie van beheersystemen voor informatiebeveiliging en volgens professor Edward Humphreys, coördinator van de ISO 2700x-normen, "*een beheerkader biedt voor de evaluatie van en de omgang met al dan niet cybergerichte risico's die bedrijven en overheden schade kunnen berokkenen of zelfs de nationale basisinfrastructuur van een land kunnen beschadigen*" [7]
- de norm ISO/CEI 27032:2012 (die momenteel wordt herzien) biedt richtlijnen voor cyberveiligheid, m.a.w. voor de bescherming van de cyberspace, die wordt gedefinieerd als "*een complexe omgeving die gebaseerd is op de onderlinge connecties tussen personen, software en diensten en mogelijk wordt gemaakt door de wereldwijde verspreiding van mechanismen en netwerken van informatie- en communicatietechnologie (ICT)*." Ter bescherming tegen aanvallen zoals manipulatie door social engineering, hacking en malware, wordt er een cyberbeveiligingsmethodologie gehanteerd die steunt op de volgende drie pijlers: opsporen, beheersen, neutraliseren

2.2. Op het niveau van de verschillende landen

Het **Groothertogdom Luxemburg** – dat al ter sprake kwam in het kader van de benchmarking aan het begin van dit hoofdstuk – publiceerde in 2015 de tweede versie van zijn Nationale strategie inzake cyberveiligheid ,[8] amper drie jaar na de verschijning van de eerste versie. De autoriteiten van het Groothertogdom maken gebruik van verschillende kanalen om de doelgroepen, met name de bedrijven en de burgers, te informeren en sensibiliseren. In de herziene versie van 2015 heeft Luxemburg in zijn cyberbeveiligingsstrategie de definitie van de ITU overgenomen.

5 Europese Commissie, Directoraat-generaal Communicatienetwerken, Inhoud en Technologie. Voorstel voor een verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie («de cyberbeveiligingsverordening»). Cybersecurity Package, website van de Europese Commissie, online (geraadpleegd op 16/02/2018). Zie https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en.

6 Internationale Organisatie voor Standaardisatie. L'ISO fête ses 70 ans ! (De ISO wordt 70!) Persbericht. Archives, Actualités, website van de ISO, online (geraadpleegd op 16/02/2018). Zie https://www.iso.org/fr/news/2017/02/Ref2163.html.

7 HUMPHREYS, Edward. La nouvelle cyberguerre. (De nieuwe cyberoorlog) Archives, Actualités, website van de ISO, oktober 2013 online (geraadpleegd op 16/02/2018). Zie https://www.iso.org/fr/news/2013/10/Ref1785.html.

8 Regering van het Groothertogdom Luxemburg, Nationaal ministerie Hoog Commissariaat Nationale Bescherming. Nationale strategie inzake cyberbeveiliging II. Cyber- en informatiebeveiliging, website van de Regering vond het Groothertogdom Luxemburg, online (geraadpleegd op 16/02/2018). Zie https://cybersecurite.public.lu/fr/securite-information/strategie-nationale.html.

In de **Verenigde Staten** stemt de officiële definitie van cyberbeveiliging [9] deels overheen met deze die werd goedgekeurd door de ITU. Ze wordt gebruikt door alle federale agentschappen voor: "*het voorkomen van schade aan, het beschermen van en het herstellen van zowel computers, elektronische communicatiesystemen en -diensten, kabelcommunicatie en elektronische communicatie als de hierin opgeslagen informatie om de beschikbaarheid, integriteit, authenticatie, vertrouwelijkheid en onweerlegbaarheid ervan te garanderen*".

Bij monde van het Nationaal Cyber Security Centrum (NCSC), dat afhangt van het Nederlands ministerie van Justitie en Veiligheid geldt in **Nederland** de volgende definitie [10]: "*Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De ICT-schade kan bestaan uit aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.*"

In **Frankrijk** definieert het Nationaal agentschap voor de beveiliging van de informatiesystemen (ANSSI), dat onder de bevoegdheid valt van de secretaris-generaal voor defensie en nationale veiligheid die de eerste minister bijstaat in de uitoefening van zijn bevoegdheden inzake defensie en nationale veiligheid definieert cyberveiligheid als "*de streeftoestand van een informatiesysteem, waarin het bestand is tegen voorvallen die hun oorsprong vinden in cyberspace en die de beschikbaarheid, de integriteit of de vertrouwelijkheid in gevaar kunnen brengen van de opgeslagen, verwerkte of verzonden gegevens of de daaraan gerelateerde diensten die via die informatiesystemen worden aangeboden of toegankelijk zijn.*"[11]

Estland definieert cyberveiligheid als de middelen die moeten worden ingezet om te anticiperen op potentiële dreigingen en er een passend antwoord op te bieden, ter bescherming van het land en zijn inwoners in de cyberspace. De cyberbeveiligingsstrategie valt er onder de bevoegdheid van het ministerie van Economische Zaken en Communicatie en is opgebouwd rond drie krachtlijnen: verdediging van kritieke infrastructuren en diensten van vitaal belang, de strijd tegen cybercriminaliteit, en landsverdediging.

3. HUIDIGE CYBERVEILIGHEIDSACTOREN EN -BELEIDSLIJNEN

Zoals ENISA benadrukt is het "*gezien de grensoverschrijdende aard van cyberdreiging van het grootste belang om de nadruk te leggen op internationaal samenwerken. Er moet samengewerkt worden op Europees niveau om paraat te kunnen staan voor en te kunnen reageren op cyberaanvallen. Integrale nationale cyberveiligheidsstrategieën zijn een eerste stap in de goede richting.*"[12]

9 United States of America, National Security Agency. Glossary. Committee on National Security Systems (CNSS), NSA, N° 4009, april 2015. Zie de blog cryptosmith.com (geraadpleegd op 16/02/2018): https://cryptosmith.com/glossary/

10 Nederlandse rijksoverheid, Ministerie van Justitie en Veiligheid, Nationaal Coördinator Terrorismebestrijding en Veiligheid. Nationale Cybersecurity Strategie 2 - Van bewust naar bekwaam. Nationale Cybersecurity Strategie, website van het ministerie van Justitie en Veiligheid, online (geraadpleegd op 16/02/2018). Zie https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie.

11 République française, Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information. (Republiek Frankrijk, Secretariaat-generaal voor defensie en nationale veiligheid, Nationaal agentschap voor de beveiliging van informatiesystemen.) Glossaire. (Woordenlijst) Glossaire, website van het ANSSI, online (geraadpleegd op 16/02/2018). Zie https://www.ssi.gouv.fr/entreprise/glossaire/c/

12 FALESSI, Nicole, GAVRILA, Razvan, KLEJNSTRUP, Ritter, MOULINOS, Konstantinos. National Cyber Security Strategies - Practical Guide on Development and Execution. Europees agentschap voor de beveiliging van netwerken en informatie, Europese Unie, 19 december 2012, online (geraadpleegd op 16/02/2018). Zie https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

Dat het gewest alleen zou handelen, is dus uitgesloten. Het gewestelijk cyberveiligheidsplan moet worden geïntegreerd in het beleid en de modellen die op federaal en Europees niveau zijn vastgelegd, en moet worden opgesteld in samenspraak met andere entiteiten van onze federale staatsstructuur.

3.1. Cyberveiligheid op Europese schaal

Cyberveiligheid maakt integraal deel uit van de initiatieven die de Europese Unie (EU) neemt om de digitale eengemaakte markt te realiseren en te versterken. De beveiliging van cyberspace is dan ook opgenomen in het Europees beleid dat ernaar streeft de hinderpalen weg te nemen om de mogelijkheden van het internet optimaal te benutten. "*Een goed functionerende digitale eengemaakte markt betekent minder belemmeringen en meer kansen*", schrijft de Europese Commissie [13], "*waardoor mensen en bedrijven vrij zaken kunnen doen en kunnen innoveren. Legaal, veilig, betrouwbaar en zonder onnodige kosten, dus in alle opzichten beter.*" Op die manier dient het cyberveiligheidsbeleid van de EU de doelstellingen inzake het handhaven van de economische activiteit en het behoud van de welvaart.

In dit kader heeft Europa in september 2017 de strategie die ze in 2013 had vastgelegd versterkt aan de hand van een cyberbeveiligingspakket dat zich concentreert op drie punten: veerkracht, ontrading en verdediging. In dezelfde lijn heeft de EU een gemoderniseerd regelgevingskader goedgekeurd met het oog op de ondersteuning van de digitale eengemaakte markt. Er zijn twee basisteksten die op dat vlak verband houden met cyberveiligheid: de Europese GDPR-verordening (General Data Protection Regulation, Algemene Verordening Gegevensbescherming) en de allereerste wetgeving met het oog op de beveiliging van de netwerk- en informatiesystemen van de lidstaten (de zogenaamde NIS-richtlijn).

DE NORMEN, PRINCIPES EN WAARDEN DIE DE EUROPESE UNIE OFFLINE VERDEDIGT MOETEN OOK ONLINE GELDEN

3.1.1. Strategie inzake cyberbeveiliging van de Europese Unie

De **Strategie inzake cyberbeveiliging van de Europese Unie** die werd gepresenteerd in 2013 en aangepast in 2017, vormt de kern van de aanpak van de Europese Commissie ter bescherming van zowel de digitale ruimte als de bedrijven en gebruikers die zich erin bewegen. Deze globale strategie wordt aangevuld met teksten over en maatregelen voor specifieke aspecten.

A. Globale aanpak: strategie inzake cyberveiligheid

In 2013 stelden de Commissie en de hoge vertegenwoordiger van de EU voor buitenlandse zaken en veiligheidsbeleid samen de Strategie inzake cyberbeveiliging van de Europese Unie voor. Die strategie beoogde een open, veilige en beveiligde cyberspace [14] voor de gebruikers en voorzag een belangrijke rol voor de overheidsinstanties.

13 Europese Commissie. Digitale eengemaakte markt - Meer ruimte voor nieuwe ontwikkelingen online. Website van de Europese Commissie, online (geraadpleegd op 30/05/2018). Zie https://ec.europa.eu/commission/priorities/digital-single-market_nl

14 Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace. Zie hoger.

Vier jaar later stelde de voorzitter van de Europese Commissie in zijn State of the Union in september 2017 vast dat ondanks de "*duidelijke vooruitgang [die is] geboekt wat betreft de veiligheid van de Europese burger online [...] Europa nog steeds niet goed gewapend is tegen cyberaanvallen*" [15], en riep hij op tot een betere bescherming van de Europese burger in het digitale tijdperk.

Op basis van die oproep heeft de Europese Commissie een nieuw cyberbeveiligingspakket voorgesteld als aanpassing en versterking van haar strategie van 2013, met name op drie kerngebieden:

- het consolideren van de **veerkracht** van de EU ten aanzien van cyberaanvallen, en de verhoging van haar reactievermogen op het vlak van cyberbeveiliging
- het **ontmoedigen** door een doeltreffende bestrijding via het strafrecht
- **verdediging** door meer stabiliteit op wereldwijde schaal via internationale samenwerking

In het kader hiervan heeft de commissie de volgende maatregelen aangekondigd:

- uitbreiding van het mandaat van het EU-agentschap voor netwerk- en informatieveiligheid (ENISA) tot een echt cyberbeveiligingsagentschap [16]
- invoering van een certificeringssysteem inzake cyberbeveiliging op EU-schaal
- invoering van een actieplan inzake de responsmogelijkheden bij grootschalige incidenten en crisissituaties inzake cyberveiligheid
- oprichting van een Europees onderzoeks- en competentiecentrum voor cyberveiligheid
- snelle toepassing van de Europese richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn [17])

Deze nieuwe maatregelen komen boven op de **initiële prioriteiten en principes van de Strategie inzake cyberbeveiliging van de EU** die worden samengevat in de onderstaande tabel:

KRACHTLIJNEN VAN DE STRATEGIE INZAKE CYBERBEVEILIGING VAN DE EUROPESE UNIE

5 STRATEGISCHE PRIORITEITEN:	5 CYBERVEILIGHEIDSPRINCIPES:
• werken aan de cyberveerkracht • cybercriminaliteit aanzienlijk terugdringen • een cyberdefensiebeleid en aanverwante middelen ontwikkelen gekoppeld aan het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) • industriële en technologische hulpmiddelen voor de cyberveiligheid ontwikkelen • een coherent internationaal cyberspacebeleid van de Europese Unie invoeren en de kernwaarden van de EU bevorderen	• de EU-kernwaarden gelden in de virtuele wereld evenzeer als in de reële wereld • bescherming van de grondrechten, vrijheid van meningsuiting, persoonsgegevens en persoonlijke levenssfeer • toegang voor iedereen • participatief, democratisch en doeltreffend bestuur • gedeelde verantwoordelijkheid voor de veiligheid

15 JUNCKER, Jean-Claude. Toespraak over de staat van de Unie 2017. Toespraak. Voorzitterschap, Europese Commissie, Brussel, 13 september 2017, online (geraadpleegd op 30/05/2018). Zie http://europa.eu/rapid/press-release_SPEECH-17-3165_nl.htm.

16 Meer hierover leest u op pagina 32.

17 Verderop, op pagina 26, gaan we dieper in op de NIS-richtlijn

B. Gerichte aanpak: teksten en maatregelen als aanvulling op de Strategie inzake cyberbeveiliging van de EU

In april 2015 stelde de Europese Commissie haar **veiligheidsprogramma** voor **voor de periode tot 2020** [18] voor. Het programma biedt met name een antwoord op de toenemende ongerustheid over terrorisme bij de Europese burgers. Het doel is een betere en nauwere samenwerking tussen de lidstaten op basis van drie prioriteiten, waaronder cybercriminaliteit. Een van de belangrijkste acties voorziet het versterken van de instrumenten in de strijd tegen cybercriminaliteit, en streeft naar het verhelpen van *"de hindernissen bij online strafrechtelijk onderzoek. Daarbij gaat het met name om het bepalen van de bevoegde rechterlijke instantie en om regelgeving inzake de toegang tot bewijsmateriaal en informatie op internet."*

In mei 2015 lanceerde de Europese Commissie haar **Strategie voor een digitale eengemaakte markt** [19] die ernaar streeft meer ruimte te maken voor nieuwe online ontwikkelingen. Een van de grootste hinderpalen is de cyberdreiging.

Voor de commissie draait het hier om de online-economie en in bredere zin de welvaart te verdedigen. De commissie heeft de volgende doelen:

- zorgen voor meer capaciteit en samenwerking
- van de Europese Unie een speler van formaat maken
- cyberbeveiliging integreren in EU-beleidslijnen

Tot slot kondigde de Europese Commissie in juli 2016 de lancering van een **publiek-privaat partnerschap (PPP) op het gebied van cyberbeveiliging** [20] aan dat past in de strategie inzake de digitale eengemaakte markt. In het kader van het onderzoeks- en innovatieprogramma Horizon 2020 gaat de EU 450 miljoen euro in dit partnerschap investeren. Verwacht wordt dat de privésector, die in het PPP wordt vertegenwoordigd door de European Cyber Security Organisation (ECSO, Europese organisatie voor cyberbeveiliging) [21], nog eens drie keer dat bedrag investeert. Bij het PPP zouden ook onderzoekscentra, universiteiten en nationale, regionale en lokale overheden worden betrokken. Het doel van het partnerschap is de samenwerking in de beginfase van het onderzoeks- en innovatieproces aan te zwengelen en cyberbeveiligingsoplossingen te ontwikkelen voor diverse sectoren, waaronder de energie-, gezondheidszorg-, vervoers- en financiële sector. De eerste oproepen tot voorstellen zijn eind 2016 gelanceerd.

18 Europese Commissie. Commissie bevordert EU-samenwerking in strijd tegen terrorisme, georganiseerde misdaad en cybercriminaliteit. Persbericht. Persberichten, Europese Commissie, 28 april 2015, Straatsburg, online (geraadpleegd op 31/05/2018). Zie http://europa.eu/rapid/press-release_IP-15-4865_nl.htm.

19 Europese Commissie. Digital Single Market. Website van de Europese Commissie, online (geraadpleegd op 16/02/2018). Zie https://ec.europa.eu/digital-single-market

20 Europese Commissie. Commissie sluit overeenkomst over cyberbeveiliging met het bedrijfsleven en voert inspanningen tegen cyberdreigingen op. Persbericht. Persberichten, Europese Commissie, 5 juli 2016, Brussel, online (geraadpleegd op 31/05/2018). Zie http://europa.eu/rapid/press-release_IP-16-2321_nl.htm.

21 Kijk voor meer informatie over de Europese organisatie voor cyberbeveiliging op de website www.ecs-org.eu

3.1.2. Nieuw EU-regelgevingskader: NIS-richtlijn en GDPR-verordening

Er zijn twee nieuwe EU-basisteksten [22] die onlangs een nieuw kader hebben geschapen voor gegevensbescherming en in deze context in nauw verband staan met cyberveiligheid:

A. de allereerste gemeenschappelijke wetgeving inzake cyberbeveiliging die moet bijdragen tot het handhaven van de **beveiliging van netwerk- en informatiesystemen** van de EU-lidstaten, met name richtlijn (EU) 2016/1148 van 6 juli 2016 [23], bekend onder de naam NIS-richtlijn (voor "Network and Information Systems")

B. de Europese GDPR-verordening ("General Data Protection Regulation", in het Nederlands ook bekend onder de afkorting AVG, Algemene Verordening Gegevensbescherming) die moet zorgen voor de uniformering en versterking van de **bescherming van persoonsgegevens en de eerbiediging van de persoonlijke levenssfeer in het kader van elektronische communicatie**, om de burgers zelf de controle over hun gegevens te geven

Dit Europees regelgevend kader heeft betrekking op een zeer grote groep personen en entiteiten, van consumenten tot leveranciers van onlinediensten en openbare diensten [24].

A. De NIS-richtlijn, Europees kader voor de organisatie van de beveiliging van netwerk- en informatiesystemen

De Europese NIS-richtlijn [25] inzake de beveiliging van netwerk- en informatiesystemen schept een wettelijk kader dat de lidstaten moet helpen om het algemene cyberbeveiligingsniveau in de EU te verhogen.

De NIS-richtlijn is opgebouwd rond 3 krachtlijnen:

- de lidstaten stimuleren om zich voor te bereiden door hen te verplichten om passende instrumenten in het leven te roepen, meer bepaald een computer security incident response team (CSIRT, responsteam dat wordt ingeschakeld bij computerbeveiligingsincidenten) en nationaal bevoegde cyberveiligheidsautoriteit
- de lidstaten laten samenwerken door de oprichting van een samenwerkingsgroep en een CSIRT-netwerk om die samenwerking vlotter te laten verlopen
- een veiligheidscultuur stimuleren binnen de sectoren die van vitaal belang zijn voor de economie en vooral binnen sectoren die intensief gebruikmaken van ICT, waarbij ondernemingen in de lidstaten die worden beschouwd als aanbieders van essentiële diensten en leveranciers van digitale diensten worden verplicht om bepaalde vereisten na te leven op het vlak van zowel beveiliging tegen incidenten als melding van ernstige incidenten

22 Europese Commissie. Digital Single Market - Making the most of the digital opportunities in Europe. Factsheet. Grafische voorstelling. News, Digital Market, Europese Commissie, 24 februari 2017, online (geraadpleegd op 22/12/2017). Zie https://ec.europa.eu/digital-single-market/en/news/digital-single-market-making-most-digital-opportunities-europe

23 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie. Deze richtlijn is in werking getreden op 8 augustus 2016 en moest door de lidstaten uiterlijk op 9 mei 2018 worden overgenomen in hun nationale rechtsorde. Zie http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016L1148&qid=1497256687970

24 Kijk voor meer informatie over de verplichtingen van de openbare diensten naar het kaderstuk op pagina 31 "De regels naleven: hoe kan het CIBG helpen?".

25 Een richtlijn is een van de "juridische instrumenten die de Europese instellingen tot hun beschikking hebben om het beleid van de Europese Unie (EU) ten uitvoer te leggen. Ze is een flexibel instrument dat vooral gebruikt wordt als middel om nationale wetten te harmoniseren. EU-landen worden erdoor verplicht bepaalde resultaten te bereiken, maar ze mogen daarbij zelf bepalen hoe ze dat doen." Bron: EUR-LEX, http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=URISERV%3Al14527

Meer bepaald moeten we naast de definities die de richtlijn biedt, de verplichtingen onthouden die ze oplegt. Enkele hoofdpunten:

- De beveiliging van netwerk- en informatiesystemen is het "vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar te brengen".
- Aanbieders van essentiële diensten (waaronder eventueel overheidsinstanties) moeten:
  - "*passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, te beheersen*";
  - "*passende maatregelen nemen om de gevolgen van incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en te minimaliseren om de continuïteit van deze diensten te waarborgen*".

DE KRITIEKE INFRASTRUCTUREN VOLGENS DE NIS-RICHTLIJN

SECTOR	DEELSECTOR
Energie	Elektriciteit
	Aardolie
	Aardgas
Vervoer	Luchtvervoer
	Spoorwegvervoer
	Vervoer via waterwegen
	Wegvervoer
Banken	
Infrastructuren van financiële markten	
Zorgsector	Zorginstellingen (waaronder ook privéziekenhuizen en -klinieken)
Aanvoer en distributie van drinkwater	
Digitale infrastructuren	

De NIS-richtlijn in België

OP FEDERAAL NIVEAU

Het **Centrum voor Cybersecurity België (CCB)** [26] heeft van de federale overheid de opdracht gekregen om de wetgeving voor te bereiden die de NIS-richtlijn moet omzetten in nationaal recht. Daartoe heeft het CCB een algemeen omzettingskader voor de richtlijn in België uitgewerkt dat het op 30 maart 2018 heeft voorgelegd aan de federale Ministerraad als een voorontwerp van wet [27]. Het voorontwerp van de omzettingswet, dat werd goedgekeurd door de federale regering en ter advies wordt voorgelegd aan de Raad van State, voorziet in de aanstelling van "*bevoegde overheden op twee niveaus en met verschillende rollen*", met name een nationale overheid en sectorale overheden. De sectorale overheden zouden voor hun respectieve sectoren worden belast met de identificatie van de aanbieders van essentiële diensten (AED's) in het kader van de NIS-richtlijn.

In het kader van zijn voorbereidende werkzaamheden [28] had het CCB:

- het begrip AED als volgt gedefinieerd: "*een entiteit die een voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten essentiële dienst verleent*", waarbij de verlening van die dienst "*afhankelijk is van netwerk- en informatiesystemen*" en een incident in dat kader een gebeurtenis is die "*aanzienlijke verstorende effecten zou hebben voor de verlening van die dienst*";
- voorgesteld :
  - om de **overheid** op te nemen in de lijst van AED's;
  - om een **beroep te doen op sectorale overheden** voor elke betrokken sector, waarbij die overheden moeten samenwerken met het CCB om aanbieders van essentiële diensten en leveranciers van digitale diensten te identificeren, beveiligingsnormen vast te leggen en die aanbieders en leveranciers te controleren;
  - dat het CCB de aangestelde sectorale overheden, de **gewest- en gemeenschaps-overheden** en de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken zou raadplegen met het oog op het bepalen van de gemeenschappelijke criteria voor alle sectoren (= transsectoraal) voor de identificatie van aanbieders van essentiële diensten, waarbij elke sectorale overheid de mogelijkheid krijgt om voor de eigen sector specifieke criteria toe te voegen;
  - om te komen tot een gemeenschappelijk, algemeen pakket van beveiligingsmaatregelen voor netwerk- en informatiesystemen, op basis van **internationale standaarden** en dus in informatietechnologiebeveiligingsmiddens erkende **specifieke regels** (ISO2700X en andere normen);
  - dat een onafhankelijk organisme **controles op de verplichtingen van de AED's** zou verzorgen en dat de sectorale overheden ook verzoeken zouden kunnen uitvaardigen tot het voldoen aan de regels binnen een bepaalde termijn en/of sancties zouden kunnen opleggen.

26 Zie rubriek 1.2.2 "Op Belgisch niveau" op pagina 34 voor de rol en de werking van het Centrum voor Cybersecurity België.
27 Koninkrijk België, FOD Kanselarij van de Eerste Minister. Kader voor de beveiliging van netwerk- en informatiesystemen voor de openbare veiligheid. Persbericht. Ministerraad van 30 maart 2018, Presscenter.org, online (geraadpleegd op 31/05/2018). Zie http://www.presscenter.org/nl/pressrelease/20180330/kader-voor-de-beveiliging-van-netwerk-en-informatiesystemen-voor-de-openbare-v
28 Koninkrijk België, FOD Kanselarij van de Eerste Minister. Algemeen omzettingskader van de NIS-richtlijn in België. Persbericht. Ministerraad van 20 juli 2017, Presscenter.org, online (geraadpleegd op 31/05/2018). Zie http://www.presscenter.org/nl/pressrelease/20170720/algemeen-omzettingskader-van-de-nis-richtlijn-in-belgie.

De NIS-richtlijn in België

OP HET NIVEAU VAN HET BRUSSELS HOOFDSTEDELIJK GEWEST

Het Brussels Hoofdstedelijk Gewest moet zijn medewerking verlenen aan de werkzaamheden voor de omzetting van de NIS-richtlijn. Het CIBG en BPV zijn op dat vlak kritieke spelers en zeer geschikt als gewestelijke gesprekspartners van het CCB. De in hoofdstuk 3 van dit katern voorgestelde maatregelen passen binnen deze dynamiek [29].

B. Algemene Verordening Gegevensbescherming (AVG)

De **Europese GDPR-verordening** [30] komt voort uit de wens van de EU om bij de Europese burgers een klimaat van vertrouwen te scheppen met betrekking tot het gebruik van hun persoonsgegevens, d.w.z. alle gegevens waarmee een natuurlijke persoon kan worden geïdentificeerd [31]. Daarmee streeft de verordening een economisch doel na: de activiteiten van bedrijven in het kader van de digitale eengemaakte markt vlotter laten verlopen. De verordening wil ook een verdedigingswal optrekken tegen cyberaanvallen via de verplichtingen bij het verzamelen, bewaren en/of bewerken van persoonsgegevens.

Door de aanhoudende technologische evolutie moest de bestaande wetgeving nodig herzien worden, want door de eengemaakte grote markt waarin het internet de grenzen had vervaagd, was ze verouderd of zelfs compleet achterhaald. We hebben het dan over zowel de richtlijn van 1995 inzake de gegevensbescherming met het oog op de eerbiediging van de persoonlijke levenssfeer als het kaderbesluit van 2008 dat de samenwerking tussen de politie- en gerechtelijke diensten betrof.

Met de GDPR beschikt de EU nu over een uniform wettelijk kader volgens het principe 'één continent, één wet', met maatregelen die gelden voor alle gegevensbeheerders, waar ze ook gevestigd zijn, zelfs als dat buiten Europa is. De verordening is in werking getreden op 27 april 2016 en voorzag in een termijn van twee jaar om alle betrokkenen de kans te geven zich aan de nieuwe eisen aan te passen, dus tot 25 mei 2018.

Persoonsgegevens en de bescherming ervan volgens de GDPR

De in de GDPR opgenomen definitie van persoonsgegevens is zeer breed. Ze omvat alle informatie over een geïdentificeerde of identificeerbare levende natuurlijke persoon, waaronder informatie met betrekking tot diens fysieke, fysiologische en mentale toestand, en genetische, biometrische, medische, economische, culturele en sociale gegevens. Ook IP-adressen, cookies en RFID-tags vallen onder deze definitie.

Concreet legt de verordening de rechten van de burgers vast op verschillende niveaus die ook raakpunten hebben met cyberbeveiliging:

- **gegevensbescherming door standaardinstellingen en door ontwerp** (of 'privacy by default' en 'privacy by design' in het Engels) is een van de basisprincipes van de verordening en waarborgt dat:

29 Zie pagina 45 en volgende.
30 Verordeningen zijn rechtshandelingen. Ze zijn van algemene toepassing, in al hun onderdelen bindend en rechtstreeks toepasselijk in alle landen van de Europese Unie. Bron: EUR-LEX, http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=LEGISSUM:l14522
31 Conform de GDPR vallen onder de definitie van persoonsgegevens alle gegevens over een geïdentificeerde of identificeerbare levende natuurlijke persoon, waaronder informatie met betrekking tot diens fysieke, fysiologische en mentale toestand, en genetische, biometrische, medische, economische, culturele en sociale gegevens.

- elke dienst die gebruikmaakt van persoonsgegevens daar automatisch het hoogste beschermingsniveau op toepast;
- de wetgeving preventief en proactief geldt voor alle mogelijke nieuwe technologieën.

- verwerkingsverantwoordelijken hebben de plicht om **de burger en de autoriteiten onverwijld op de hoogte te brengen** wanneer gegevens per ongeluk of onrechtmatig vernietigd worden, verloren gaan, gewijzigd worden, door niet-bevoegde personen worden ingekeken of aan deze personen worden meegedeeld en wanneer de rechten van de betrokkenen in gevaar zijn;
- strenge **beperkingen inzake het verzamelen, verwerken en bewaren van gegevens** verminderen de facto de risico's:
  - persoonsgegevens worden verzameld voor een specifiek gerechtvaardigd doel en mogen niet voor andere doeleinden worden gebruikt;
  - alleen de gegevens die noodzakelijk zijn voor de voorgenomen doeleinden mogen worden verzameld;
  - persoonsgegevens worden niet langer bewaard dan nodig om het doel te bereiken;
  - persoonsgegevens moeten worden beschermd tegen elk(e) ongeoorloofd(e) inzage, verlies of vernietiging.

Cyberveiligheid en in het bijzonder de opsporing van en respons op cyberdreiging die moeten getuigen van de nodige cyberveerkracht, maken impliciet deel uit van de AVG. De verplichting om de burger en de autoriteiten op de hoogte te brengen bij gegevensinbreuken houdt verband met de respons op cyberdreiging. De verplichtingen van entiteiten die gegevens bezitten, beperken zich op dat vlak niet tot de bovenstaande bepalingen. De verordening legt ook een verantwoordingsbeginsel vast ('accountability') dat inhoudt dat de entiteit die verantwoordelijk is voor de gegevens:

- maatregelen moet hanteren om de persoonsgegevens te beschermen tegen elk(e) ongeoorloofd(e) inzage, verlies of vernietiging;
- moet kunnen aantonen dat ze overeenkomstig de AVG handelt.

De AVG legt dus wel degelijk verplichtingen op die verband houden met cyberveerkracht.

De regels naleving: hoe kan het CIBG hierbij helpen?

Net als andere wetten hebben ook de NIS-richtlijn en de GDPR-verordening al dan niet rechtstreeks impact op de organisatie van de openbare diensten. Daarom biedt het CIBG de openbare besturen en instellingen een hele waaier van diensten om hen te helpen aan de wettelijke regels te voldoen.

- **NIS en informatiebeveiliging**: zonder te wachten tot het toepassingsgebied van de NIS-richtlijn wordt afgebakend en tot de AED's zijn geïdentificeerd, moeten de openbare diensten sowieso diverse verplichtingen en beste praktijken inzake informatiebeveiliging naleven.

Het CIBG beschikt sinds 2010 over een dienst die zich toespitst op informatiebeveiliging en de naleving van de wettelijke voorschriften met name wat betreft de bescherming van persoonsgegevens. **De klanten van het CIBG kunnen een beroep doen op de expertise van dit team, dat hun Information Security as a Service (ISaaS) levert**.

Onder ISaaS vallen uiteenlopende prestaties, zoals informatiebeveiligingsadvies, het analyseren van het informatiebeveiligingsbeleid van de organisatie, de invoering en opvolging van bijhorende maatregelen en de permanente analyse van het informatiebeveiligingsbeleid op basis van een proces van permanente verbetering (plan – do – check – act) met de bijbehorende aanbevelingen en verbetervoorstellen.

De informatiebeveiligingsanalyses van het CIBG zijn gebaseerd op het referentiekader van de ISO 27001-norm en volgende, en worden aangevuld met risicoanalyses. Wanneer bij de klant nog geen formeel informatiebeveiligingsplan bestaat, kan ISaaS vertrekken van een analyse van de veiligheidssituatie en de bestaande risico's op het vlak van informatie om tekortkomingen op dat vlak te verhelpen.

Voorts zijn de ISaaS-medewerkers ook bevoegd om de functie te vervullen van extern **informatieveiligheidsadviseur (IVA)** als de klant die niet wenst toe te wijzen aan een interne medewerker. Conform het koninklijk besluit van 17 maart 2013 [32] ziet de IVA erop toe dat de organisatie de nodige aandacht besteedt aan informatieveiligheid via structurele, organisatorische, fysieke en technische maatregelen.

- **AVG**: de AVG geldt ook voor openbare instanties. Daarom lanceerde het CIBG in de lente van 2017 een sensibiliseringscampagne rond **AVG-naleving** door openbare instanties. Tegelijkertijd stelde het centrum zijn dienstenaanbod voor ter ondersteuning van de naleving van de nieuwe voorschriften.

In het AVG-dienstenaanbod van het CIBG wordt de nadruk gelegd op het transversale aspect van de AVG (die immers gevolgen heeft voor veel meer dan alleen informaticaprocessen). Het gaat om vier servicetypes:

1. Opleiding: van een informatiesessie met de aandachtspunten van de AVG voor de verantwoordelijken van de partners van het CIBG tot een intense meerdaagse opleiding waarin alle juridische en technische elementen aan bod komen en de bewustmaking van het personeel inzake AVG-naleving op de werkvloer

32 Koninkrijk België, FOD Informatietechnologie en Communicatie. Koninklijk besluit betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator - 17 maart 2013. Belgisch Staatsblad, 183e jaargang, nr. 89, 22 maart 2013, Brussel, online (geraadpleegd op 16/02/2018). Zie http://www.ejustice.just.fgov.be/mopdf/2013/03/22_1.pdf#Page6

2. Een voorafgaande evaluatie om de maturiteit van de organisatie van de partner van het CIBG te beoordelen, waarbij de voornaamste gegevensverwerkingstypes en de grootste struikelblokken op het vlak van AVG-naleving worden geïdentificeerd, waarop er een verslag wordt opgesteld met de belangrijkste risicozones en een eerste versie van een actieplan op hoog niveau met het oog op AVG-conformiteit

3. Begeleiding op weg naar conformiteit door een projectleider die de AVG goed kent en wordt bijgestaan door een team dat de taken beheerst van een Data Protection Officer om een volgorde van prioriteiten te bepalen in de probleemgebieden inzake AVG-naleving en deze een voor een aan te pakken

4. Data Protection Officer (DPO) 'as a service' [33]: het CIBG kan voor zijn partners de rol van DPO en alle bijhorende verantwoordelijkheden opnemen, waaronder informatieverstrekking, coaching, advies, opleiding en controle van de AVG-naleving, en optreden als contactpersoon voor de toezichthoudende autoriteit. Elk bestuur moet immers over zo'n DPO beschikken. De DPO's van het CIBG werken in een multidisciplinair team samen met juristen, informatieveiligheids- en informatica-experts. Ze beschikken over ervaring en hulpmiddelen die precies kunnen worden afgestemd op de noden van de partnerorganisaties van het CIBG.

Verschillende gewestelijke en plaatselijke besturen hebben al gebruikgemaakt van de sensibiliserings- en opleidingssessies rond de AVG.

Meer weten? Het CIBG heeft een brochure gepubliceerd onder de titel 'Algemene Verordening Gegevensbescherming (AVG) - Praktische gids voor de gemeentelijke en gewestelijke instellingen van het Brussels Hoofdstedelijk Gewest', die u kunt downloaden op de website van het centrum [34].

3.2. Belangrijkste spelers in de cyberbeveiliging

3.2.1. Op Europees niveau:

Op Europese schaal zetten verschillende instanties zich ten behoeve van de EU-lidstaten in op het vlak van cyberbeveiliging, namelijk:

- het European Network and Information Security Agency (ENISA)
- het netwerk van nationale responsteams die worden ingeschakeld bij computerbeveiligingsincidenten (CSIRT-netwerk)
- het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3)

Daarnaast beschikt de Europese Unie over een intern CERT (CERT-EU) dat de Europese instellingen moet bijstaan in geval van een cyberaanval teneinde de integriteit van de informaticastructuren te beschermen.

33 Kijk voor meer informatie op https://cibg.brussels/nl/nieuws_publicaties/nieuws/europese-verordening-betreffende-de-bescherming-van-persoonsgegeven-avg

34 Voor meer informatie over de toepassing van de GDPR door overheidsinstanties kunt u een kijkje nemen in de brochure van het CIBG onder de titel Algemene Verordening Gegevensbescherming (AVG) - Praktische gids voor de gemeentelijke en gewestelijke instellingen van het Brussels Hoofdstedelijk Gewest. Zie http://cibg.brussels/gdpr-gids

Het ENISA, toekomstig EU-agentschap voor cyberbeveiliging

In september 2017 maakte de Europese Commissie de intentie bekend om te beschikken over een EU-agentschap voor cyberbeveiliging via de uitbreiding van het werkterrein en de opdrachten van het in 2004 opgerichte European Network and Information Security Agency (afgekort ENISA).

De oprichting van dit agentschap, voorgesteld als een van de maatregelen in het cyberbeveiligingspakket [35] van de Europese Commissie, moet de EU de mogelijkheid geven om een actievere rol te spelen in de strijd tegen cyberdreigingen. Het mandaat van het ENISA is immers te beperkt gebleken, zeker in verhouding tot de evolutie van de cyberveiligheidsnoden, in het bijzonder in de strijd tegen grootschalige cyberaanvallen.

Tot hiertoe "*ondersteunt [het Enisa] de Europese instellingen, de lidstaten en het bedrijfsleven bij het aanpakken van, reageren op en met name het voorkomen van problemen inzake netwerk- en informatiebeveiliging*". [36] In de praktijk speelt het voornamelijk de rol van expert en facilitator in de ontwikkeling van een cultuur rond de beveiliging van de informatienetwerken in de hele unie, door beste praktijken samen te brengen en stakeholders met elkaar in contact te brengen. Zo publiceert het ENISA jaarlijks het 'ENISA Threat Landscape' met een stand van zaken van de voornaamste cyberdreigingen binnen Europa.

Het **actiegebied van het toekomstige agentschap voor cyberbeveiliging** moet er het "*referentiepunt in het cyberbeveiligingsecosysteem van de EU [van maken], waarbij het nauw samenwerkt met alle andere relevante instanties binnen dat ecosysteem.*" Op dat vlak stelt de Europese Commissie vast dat "*voor het versterken van de gezamenlijke cyberweerbaarheid van de unie afzonderlijke acties door de EU-lidstaten en een versnipperde aanpak van de cyberbeveiliging niet afdoende zullen zijn*" [37].

Bij de nieuwe actiedomeinen van het toekomstige agentschap voor cyberbeveiliging horen met name:

- ontwikkeling en uitvoering van EU-beleid, waaronder de herziening van de EU-cyberbeveiligingsstrategie
- respons in geval van cyberbeveiligingscrises via samenwerking tussen de lidstaten
- ondersteuning van de NIS-richtlijn
- ondersteuning van de markt voor cyberveiligheid via de harmonisering van de nationale certificeringen voor ICT-beveiligingsproducten en -diensten
- verbetering van het kunnen en kennen van overheidsinstanties op EU- en lidstaatniveau wat de reactie op incidenten en de regelgeving betreft
- kennis- en informatie-uitwisseling en voorlichting in overleg met de autoriteiten van de lidstaten
- onderzoeks- en ontwikkelingsprioriteiten stellen, onder meer in het kader van het contractuele publiek-private partnerschap voor cyberbeveiliging

35 Zie hoger op pagina 23.
36 Voorstel voor een verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging. Zie hoger.
37 Idem

CSIRT-netwerk

Het CSIRT-netwerk is in het leven geroepen krachtens de NIS-richtlijn naar aanleiding van de wens van de Europese Commissie om een kader te scheppen voor vrijwillige samenwerking tussen EU-lidstaten. Het netwerk moet het delen van technische informatie over risico's en kwetsbare punten bevorderen. Daarvoor moet het beschikken over de effectieve, doeltreffende en beveiligde medewerking van de nationale CSIRT's van alle EU-lidstaten.

De WannaCry-cyberaanval in mei 2017 was het eerste incident waarvoor het netwerk werd ingezet, al bleek dat weinig doeltreffend, zoals de Commissie concludeerde. Daarbij merkte ze op dat dit "*incident [heeft uitgewezen] dat het systeem nog niet volledig operationeel was*" [38].

Het European Cybercrime Centre (EC3)

Het Europees Centrum voor de bestrijding van cybercriminaliteit (European Cybercrime Centre - EC3) is in 2013 opgericht binnen Europol, het Europees agentschap gespecialiseerd in de strijd tegen criminaliteit. Cybercriminaliteit maakt immers deel uit van de negen prioritaire thema's van Europol (naast onder meer de strijd tegen drugs- en mensenhandel).

EC3 heeft als opdracht de politierespons op cybercriminaliteit in de Europese Unie te versterken. Het centrum moet de lidstaten en de EU-instellingen in staat stellen om hun operationele en analytische capaciteit voor onderzoek en samenwerking met internationale partners op te voeren [39].

3.2.2. Op Belgisch niveau

In België zijn er verschillende officiële organisaties belast met cyberbeveiligingsvraagstukken afhankelijk van hun specifieke bevoegdheden en actieniveaus.

Het gaat om:

- het Centrum voor Cyberveiligheid België (CCB)
- het federaal Cyber Emergency Team (CERT.be)
- de Federal Computer Crime Unit (FCCU) en de vijf Regional Computer Crime Units (RCCU's) binnen de Belgische Federale Politie

Daarnaast is er de Cyber Security Coalition, een platform voor de samenwerking tussen overheids-, privé- en academische organisaties ter bevordering van cyberveiligheid en goede praktijken.

38 Europese Commissie. Veiligheidsunie: Commissie zet vaart achter maatregelen ter voorkoming van radicalisering en cyberdreigingen. Persbericht. Persberichten, Europese Commissie, 29 juni 2017, Brussel, online (geraadpleegd op 31/05/2018). Zie http://europa.eu/rapid/press-release_IP-17-1789_nl.htm. + Europese Commissie. Achtste voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Mededeling van de Commissie aan het Europees Parlement, de Europese Raad en de Raad. 29 juni 2017, Brussel, online (geraadpleegd op 31/05/2018). Zie http://ec.europa.eu/transparency/regdoc/rep/1/2017/NL/COM-2017-354-F1-NL-MAIN-PART-1.PDF

39 Europese Commissie. De EU-interneveiligheidsstrategie in actie. Mededeling van de Commissie aan het Europees Parlement en de Raad. 22 november 2010, Brussel, online (geraadpleegd op 31/05/2018). Zie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:NL:PDF

Het Centrum voor Cyberveiligheid België

In 2015 werd het Centrum voor Cyberveiligheid België (CCB) [40] opgericht, dat onder het gezag staat van de eerste minister.

Als nationale autoriteit heeft het CCB als opdracht:

- het opvolgen en het coördineren van, en toezien op de uitvoering van het Belgisch cyberveiligheidsbeleid
- op basis van een geïntegreerde en gecentraliseerde aanpak de projecten ter zake beheren
- de coördinatie verzorgen tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector
- het formuleren van voorstellen tot aanpassing van het regelgevend kader op het vlak van cyberveiligheid
- in samenwerking met het Coördinatie- en Crisiscentrum van de federale regering het crisisbeheer bij cyberincidenten verzorgen
- het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen
- het coördineren van de Belgische vertegenwoordiging op internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen vanaf het nationale standpunt
- het coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen
- het informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen

Met het oog op het crisismanagement bij cyberincidenten werkt het CCB aan de opstelling van een **nationaal cybernoodplan voor België** dat gericht is op "*het organiseren van een antwoordstructuur op de cybersecuritycrisissen en incidenten die een coördinatie en/of beheer op nationaal niveau vereisen.*" In het plan wordt er een mechanisme van "*basisescalatie uitgewerkt zodat de verschillende diensten actief in het cyberdomein onderlinge acties bij het behandelen van nationale cyberincidenten op elkaar afstemmen. Er wordt veel belang gehecht aan het snel en correct uitwisselen van informatie tussen de diensten*".

Op praktisch vlak heeft het CCB in januari 2017 uit hoofde van zijn coördinerende rol inzake cyberbeveiliging in België (zie verderop) het beheer op zich genomen van het **federaal cyber emergency team** (CERT.be).

Het CCB heeft verschillende projecten opgestart om de cyberveiligheid van de vitale sectoren van België te versterken. Dat zijn sectoren die cruciaal zijn voor de veiligheid van de Belgische bevolking en als dusdanig zijn geïdentificeerd in lijn met de NIS-richtlijn: het gaat om energie, mobiliteit, telecommunicatie, financiën, drinkwater, volksgezondheid en de overheid. Via een gedeeld platform krijgen die sectoren toegang tot gefilterde waarschuwingen voor intrusies en andere cyberdreigingen. Zo krijgen ze snel informatie uit een betrouwbare bron en kunnen ze snel de nodige maatregelen treffen om aanvallen te neutraliseren.

40 Het CCB (www.ccb.belgium.be) is opgericht krachtens het koninklijk besluit van 10/10/2014

Het actieterrein van het CCB is dus zeer breed en reikt verder dan het federale niveau.

Met name het huidige gewestelijk cyberveiligheidsplan is te situeren in deze invloedssfeer. Het is van essentieel belang dat het Brussels Hoofdstedelijk Gewest hier ten volle bij betrokken wordt en de verspreiding ervan coördineert en verzorgt.

Het federaal Cyber Emergency Team, CERT.be

Het federaal Cyber Emergency Team (of CERT.be, www.cert.be) werd opgericht in 2009 en is belast met de coördinatie van de aanpak en het beantwoorden van incidenten en crisissituaties van nationale omvang bij exploitanten van kritieke infrastructuren of aanbieders van essentiële diensten.

De taken van CERT.be zijn:

- informatie verzamelen en geven over veiligheidsincidenten
- ondersteuning bieden wanneer er zich incidenten voordoen
- de behandeling van grootschalige incidenten coördineren
- helpen bij het opzetten van CERT-activiteiten in de bedrijven
- gegevens en kennis delen via publicaties en events

CERT.be fungeert concreet als centraal contactpunt voor Belgische bedrijven en overheidsorganisaties bij problemen die te maken hebben met cyberbeveiliging. Zij kunnen zich tot CERT.be wenden om een cyberincident te melden en/of advies te vragen over cyberbeveiliging.

De Federal Computer Crime Unit en de Regional Computer Crime Units van de Belgische Federale Politie

De Federal Computer Crime Unit (FCCU [41]) is de eenheid van de Federale Politie die belast is met de strijd tegen ICT-gerelateerde criminaliteit. De FCCU staat met name in voor de bescherming van de burgers tegen nieuwe vormen van criminaliteit in de virtuele samenleving. De eenheid behandelt criminele feiten in cyberspace die onderhevig zijn aan strafrechtelijke vervolging zoals pedofiliedossiers, internetfraude (bedrieglijke verkoop) en oplichting via telecommunicatiekanalen.

De Regional Computer Crime Units (RCCU's) zijn werkzaam in de rechtsgebieden van de Belgische hoven van beroep [42], waaronder het gerechtelijke arrondissement Brussel. Naast onderzoek naar inbreuken die te maken hebben met internetcriminaliteit en identificatie van de daders, voeren de RCCU's ook forensische analyses van informaticasystemen uit (pc's en andere gegevensdragers en kleine netwerken).

41 Kijk voor meer informatie over de Federal Computer Crime Unit op de website http://www.politie.be/fed/nl/over-ons/centrale-directies/federal-computer-crime-unit
42 Antwerpen, Brussel, Gent, Luik en Bergen

De Cyber Security Coalition

De Cyber Security Coalition vzw (www.cybersecuritycoalition.be) is een gemeenschappelijk initiatief van de academische sector, de overheid en de privésector. De coalitie brengt meer dan 50 belangrijke spelers uit deze 3 uiteenlopende domeinen bij elkaar, opdat haar leden hun krachten kunnen bundelen om cyberveiligheid op nationaal niveau te bevorderen. Het CIBG is actief lid van de coalitie.

Dit expertnetwerk ontplooit activiteiten in vier strategische domeinen:

- delen van ervaring
- operationele samenwerking
- aanbevelingen aan de politiek
- sensibiliseringscampagnes

In 2015 publiceerde de Cyber Security Coalition de Gids voor incidentenbeheer [43] om allerlei types organisaties een antwoord te helpen vinden op de vraag: "*Is uw organisatie uitgerust om een cyberveiligheidsincident aan te pakken?*" Men vindt in de gids heel wat relevante en praktische informatie die organisaties helpt om cyberveiligheidsincidenten op te sporen en aan te pakken.

Samen met het CCB lanceerde de Cyber Security Coalition ook de campagne 'Take back the internet' via de website www.safeonweb.be, die voortvloeide uit de vaststelling dat 68% van de Belgische bevolking online niet voldoende beschermd is en het cybercriminelen dus makkelijk maakt. De campagne moedigt het grote publiek aan om toestellen te beveiligen door antivirusprogramma's te installeren, gegevens veilig te bewaren en software op tijd bij te werken. Meer dan 6,5 miljoen bezoekers hebben de test op de website al afgelegd om te kijken hoe het staat met hun beschermingsniveau.

3.2.3. Op het niveau van het Brussels Hoofdstedelijk Gewest:

In het Brusselse Hoofdstedelijk Gewest staan het Centrum voor Informatica voor het Brusselse Gewest (CIBG) en Brussel Preventie & Veiligheid (BPV) door de aard van hun taken en activiteiten al in voor diverse aspecten van cyberveiligheid op gewestelijk niveau. Voorts zijn beide partnerbesturen van plan om activiteiten te ontplooien aangaande twee strategische aspecten: de ontwikkeling van het algemeen bewustzijn inzake informatieveiligheid en de sensibilisering van partners die actief zijn in het gewest.

HET CENTRUM VOOR INFORMATICA VOOR HET BRUSSELSE GEWEST (CIBG) EN BRUSSEL PREVENTIE & VEILIGHEID (BPV) STAAN AL IN VOOR DIVERSE ASPECTEN VAN CYBERVEILIGHEID

Het CIBG en BPV onderhouden nauwe banden door verscheidene partnerships en concrete projecten zoals het gewestelijke communicatiecentrum, het gewestelijke crisiscentrum, het gewestelijke videobewakingsplatform en de implementatie van het ANPR-cameranetwerk [44]. Het CIBG is trouwens ook de IT-partner voor BPV's dagelijkse informaticabehoeften.

43 Cyber Security Coalition. Cyberveiligheid - Gids voor incidentenbeheer. Online (geraadpleegd op 31/05/2018). Zie www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-NL.pdf
44 'Automatic Number-Plate Recognition', automatische nummerplaatherkenning.

Centrum voor Informatica voor het Brusselse Gewest

Het Centrum voor Informatica voor het Brusselse Gewest (CIBG) [45] is de technologisch neutrale, competitieve, betrouwbare en hoogkwalitatieve partner van elke openbare instelling op het grondgebied van het Brussels Hoofdstedelijk Gewest die, met kennis van zaken en op proactieve wijze, vernieuwende en samenhangende ICT-technologieën wenst in te voeren, om enerzijds de eigen werking efficiënter te maken en anderzijds te zorgen voor gebruiksvriendelijke diensten voor Brusselaars, ondernemingen en bezoekers.

In het kader hiervan brengt het CIBG de plaatselijke en gewestelijke besturen samen voor projecten die hun digitale ontwikkeling stimuleren. Bundelen vormt de rode draad en tegelijkertijd de belangrijkste hefboom bij alle activiteiten van het CIBG. Dat uit zich in vier concrete krachtlijnen: bundelen van infrastructuren, ICT-platformen en -systemen, gegevens en IT-human resources.

Bovendien staat het CIBG in voor de samenhang van de organen die opgericht zijn om het IT-beleid in het Brussels Hoofdstedelijk Gewest uit te rollen. Het heeft als opdracht een permanente, doeltreffende en coherente bijdrage te leveren aan de voorbereiding van beleidslijnen, met name op basis van:

- zijn gezaghebbende en invloedrijke rol bij de bevordering van digitalisering via de ontwikkeling van de werkwijzen in openbare instellingen
- het onder de aandacht brengen en promoten van ICT
- een waakzaamheidsfunctie die grondige kennis en voortdurende observatie van de evolutie van de ICT veronderstelt inclusief het vergelijken van de eigen organisatie met andere entiteiten binnen federale structuren en met de Europese Unie

Sinds zijn oprichting is het CIBG een van de belangrijke spelers op het gebied van computerbeveiliging. Het centrum leunt van nature naar vraagstukken op het gebied van informatiebeveiliging en cyberveiligheid vanwege zowel zijn eigen behoeften als die van de organisaties die zijn diensten afnemen.

Wat informatiebeveiliging betreft, vertrouwt het CIBG in de eerste plaats op het Gewestelijk Data Center (GDC) en het IRISnet-netwerk. Het GDC, een van de pijlers van de IT-governance van de Brusselse openbare besturen, maakt dat die besturen de controle over en het beheer van hun kritieke en gevoelige gegevens kunnen handhaven. Het datacenter omvat de nodige informatica-uitrusting en servers om de gegevens van de overgrote meerderheid van de Brusselse overheidsorganisaties op plaatselijk en gewestelijk niveau te bewaren, te behandelen en te beschermen. Het GDC herbergt de centrale diensten die deel uitmaken van de gewestelijke Smart City-strategie, zoals IRISbox, dienstenintegrator Fidus en het gewestelijke videobewakingsplatform dat ondersteuning biedt aan de veiligheidsdiensten en het beheer van de Low Emission Zone. Als verantwoordelijke voor de informaticabeveiliging van het GDC staat het CIBG in contact met het CCB, dat het CIBG waarschuwt bij nieuwe dreigingen.

Klanten kunnen bovendien een beroep doen op de expertise van het CIBG om beveiligingsincidenten op te lossen. Die expertise vervolledigt het aanbod van het CIBG, dat voor een groot deel gebaseerd is op traditionele tools (firewall, back-up, Virtual Private Network) die de bescherming van systemen en gegevens waarborgen en bijdragen tot de instandhouding van de informatica-investeringen.

45 Het CIBG werd opgericht door de wet van 21 augustus 1987, zoals gewijzigd door de ordonnantie van 20 mei 1999 aangaande de reorganisatie van het CIBG en door de ordonnantie van 29 maart 2001. Tot slot wordt het CIBG in de ordonnantie van 8 mei 2014 aangeduid als gewestelijke dienstenintegrator

Tot slot fungeert het CIBG als adviseur en dienstverlener die de Brusselse overheidsorganisaties helpt zich in regel te stellen met de normen en voorschriften die al dan niet rechtstreeks verband houden met vraagstukken inzake informatiebeveiliging.

Brussel Preventie & Veiligheid (BPV)

Bij de zesde staatshervorming is de veiligheidsarchitectuur van het Brussels Hoofdstedelijk Gewest grondig hertekend. De hervorming raakt niet aan bevoegdheden en voorrechten van de verschillende beleidsniveaus (federaal/lokaal) maar heeft als voornaamste gevolg dat het Brussels Hoofdstedelijk Gewest belangrijke verantwoordelijkheden toegewezen krijgt op het vlak van preventie en veiligheid.

De hervorming heeft ertoe geleid dat de gouverneursfunctie in het Brussels Hoofdstedelijk Gewest is afgeschaft en de bevoegdheden op het vlak van veiligheid sinds 2014 in handen zijn van twee gewestautoriteiten:

- de Brusselse Minister-President, die "*de bevoegdheden uitoefent die verband houden met het handhaven van de openbare orde*"
- de Hoge Ambtenaar, die bevoegd is "*voor de gouverneurstaken die verband houden met de civiele veiligheid en voor de uitwerking van plannen met betrekking tot noodsituaties op het grondgebied van Brussel-Hoofdstad*"

Dit zijn de nieuwe taken van de Brusselse agglomeratie, die voortvloeien uit de zesde staatshervorming [46]:

- coördinatie van de veiligheidsbeleidslijnen met inbegrip van de monitoring en de registratie van de criminaliteit
- coördinatie van de preventiebeleidslijnen
- uitwerking van het gewestelijk veiligheidsplan

Voor de uitvoering van die taken heeft de Regering van het Brussels Hoofdstedelijk Gewest in het regeerakkoord 2014-2019 [47] besloten een nieuwe instelling van openbaar nut (ION) op te richten onder de naam Brussel Preventie & Veiligheid (BPV) [48].

BPV beoogt de organisatie van een gecentraliseerd en transversaal beheer van de veiligheid in Brussel en de uitbouw van een gewestelijk veiligheidsbeleid dat zijn grondslag vindt in zowel de gedecentraliseerde federale als gewestelijke bevoegdheden.

---

46 Koninkrijk België, FOD Kanselarij van de Eerste Minister. Wet met betrekking tot de Zesde Staatshervorming inzake de aangelegenheden bedoeld in artikel 77 van de Grondwet – 6 januari 2014 – Wijziging van de wet van 26 juli 1971 houdende organisatie van de agglomeraties en de federaties van gemeenten (titel hoofdstuk 2). Belgisch Staatsblad, 184e jaargang, nr. 32, 31 januari 2014, Brussel, pagina 8720, online (geraadpleegd op 31/05/2018). Zie http://www.ejustice.just.fgov.be/mopdf/2014/01/31_1.pdf. In artikel 14 worden de taken van de Brusselse agglomeratie opgenoemd. Naast de bovengenoemde bevoegdheden "oefent [de Brusselse agglomeratie] de bevoegdheden uit als bedoeld in de artikelen 128 en 129 van de provinciewet, alsook de bevoegdheden die in specifieke wetten worden toegekend aan de provinciegouverneur, behalve indien deze specifieke wetten er anders over beschikken", "oefent [ze] het toezicht uit op de begrotingen van de politiezones", "moedigt [ze] het samenvoegen van administratieve diensten van de politiezones aan, alsook het beroep door deze diensten op de aankoopcentrale voor de aankoop van materiaal" en "stelt [ze] een harmoniserende tekst voor de politiereglementen voor, met inachtneming van de specifieke kenmerken van de gemeenten".

47 Brussels Hoofdstedelijk Gewest. Regering. Brussels regeerakkoord 2014-2019. Hoofdstuk 3 – Een beleid dat de levenskwaliteit van alle wijken garandeert. § III – Een gewestelijk veiligheidsbeleid instellen (p. 67). Online (geraadpleegd op 31/05/2018). Zie http://be.brussels/files-nl/over-het-gewest/de-gewestelijke-bevoegdheden/regeerverklaring-2014-2019

48 Brussel Preventie & Veiligheid is opgericht krachtens de ordonnantie van 28 mei 2015, gepubliceerd in het Belgisch Staatsblad van 10/06/2015.

BPV vervult een centrale rol in de coördinatie van de operatoren in de preventie- en veiligheidsketen op gewestelijke schaal en zorgt voor samenhang en complementariteit door hen te verenigen binnen werkgebieden als:

- civiel crisisbeheer (politiezones en civiele veiligheidsdiensten)
- ondersteuning van de politieopleiding (Actiris, VDAB, Bruxelles Formation)
- videobewaking (politiezones, MIVB, Mobiris, CIBG)

De werking van BPV behelst zowel de preventie als aanpak van de meest uiteenlopende veiligheidskwesties rond ruimtelijke ordening, mobiliteit of andere beleidsgebieden die een weerslag hebben op de veiligheid en het veiligheidsgevoel in het Brussels Hoofdstedelijk Gewest.

Brussel Preventie & Veiligheid zorgt als koepelinstelling voor dit beleid voor het opstellen van het globaal veiligheids- en preventieplan (GVPP) [49], de coördinatie van de uitvoering en het rapporteren van de uitgevoerde maatregelen aan de bevoegde overheid. Het GVPP is opgebouwd rond tien thema's, waaronder cybercriminaliteit.

De maatregelen tegen cybercriminaliteit hebben in grote lijnen betrekking op:

- cyberhaat (M 1.2 van het GVPP)
- bewustmaking van de ICT-gerelateerde risico's (M 8.11, M 8.12, M 8.13)
- de opsporingscapaciteiten op het Darknet (M 8.14)
- het schetsen van een beeld van de cyberdreigingen en -incidenten (M 8.15)
- een technologische controlegroep voor crisisbeheer en veerkracht om een meerwaarde te kunnen bieden inzake technische en technologische innovatie (M 10.13).

Brussel Preventie & Veiligheid heeft dankzij zijn unieke positie en het opstellen van het hierboven besproken plan veranderingen op gang gebracht in de coördinatie en centralisering van het veiligheidsbeleidsbeheer in ruime zin.

Anderzijds wenst BPV bij te dragen aan de ontwikkeling van nieuwe technologieën die niet alleen in het dagelijkse leven een belangrijk hulpmiddel zijn (bereikbaarheid en beschikbaarheid van het wifinetwerk, e-loketten van bestuurlijke diensten, intelligente openbare verlichting enz.), maar ook de veiligheid van de stadsbewoners verbeteren. Van het Brussels Hoofdstedelijk Gewest een Smart City maken is een prioriteit. Het globaal veiligheids- en preventieplan moedigt innovatief onderzoek naar deze materie aan; samen met de verschillende partners van de veiligheidsketen wordt in dat opzicht nagedacht over een aangepast instrument voor informatie-uitwisseling. Zo wordt momenteel gemeenschappelijk informaticabeheer ingevoerd voor de zes politiezones (met een gedeeld videoconferentiesysteem) dat voortvloeit uit een samenwerking tussen BPV, het CIBG en de gemeenten. De uitrol van het ANPR-netwerk (Automatic Number Plate Recognition) en de Low Emission Zone op het grondgebied van het gewest is nog zo'n project waarvoor nieuwe technologieën worden ingezet en dat wordt opgevolgd door BPV en het CIBG.

49 Brussels Hoofdstedelijk Gewest, Brussel Preventie & Veiligheid. Globaal veiligheids- en preventieplan. Online (geraadpleegd op 31/05/2018). Zie http://www.veiligheid-securite.brussels/nl/plan

Ook de oprichting van een technologische controlegroep behoort tot de plannen van BPV. Dit project wordt gerealiseerd in samenwerking met de RCCU van de gerechtelijke politie van Brussel, en de controlegroep zal bestaan uit specialisten die de opdracht krijgen om technische en technologische innovaties te identificeren die een meerwaarde kunnen bieden op het vlak van crisisbeheer en veerkracht.

Om het gebruik van die nieuwe hulpmiddelen te optimaliseren en het hoofd te bieden aan de uiteenlopende vormen van criminaliteit en onveiligheid die voortdurend evolueren, is het tot slot van essentieel belang om ook de opleiding te verbeteren. De Gewestelijke School voor Veiligheidsberoepen zal in haar opleidingsaanbod oog hebben voor de professionalisering van de preventie- en veiligheidsactoren, maar ook voor het opheffen van de grenzen tussen benaderingen (uitwisseling van goede praktijken, gemeenschappelijke processen enz.). Daarnaast zal de school de overdracht van kennis en praktijken tussen de actoren aanmoedigen en trachten de kennis van de Brusselse realiteit te optimaliseren. Tot slot zal de school de synergie tussen het onderwijs, de openbare diensten voor beroepsopleiding en hun partners versterken om de expertise van de actoren te vergroten en veiligheidsberoepen aantrekkelijker te maken voor Brusselse kandidaten.

4. BESTAAND METHODOLOGISCH KADER VOOR CYBERVEILIGHEID

Er zijn enkele bestaande methodologieën die organisaties ter bestrijding van cyberrisico's en -dreigingen kunnen helpen bij het kaderen van deze bezigheden. Het gaat om:

- het Cybersecurity Framework van het National Institute of Standards and Technology in de VS
- de 2700x-normen van de Internationale Organisatie voor Standaardisatie (ISO)

4.1. Cybersecurity Framework

Het **Cybersecurity Framework** (CSF) [50] van het National Institute of Standards and Technology (NIST) is een methodologisch kader op basis waarvan bedrijven het risico op cyberaanvallen waaraan hun strategische infrastructuren blootstaan, kunnen benaderen en verwerken, en dat een context biedt waarbinnen de bedrijven beste praktijken kunnen uitwisselen op basis van een gemeenschappelijke vakwoordenschat. Het is praktisch gezien een van de meest geavanceerde modellen en daarom ook een wereldwijde referentie in zijn domein.

De aanleiding van het CSF was de reeks zware computeraanvallen waar grote bedrijven, de media, de sociale media en overheidsinstanties in de VS in 2013 mee af te rekenen kregen. Die incidenten brachten de risico's van onderbrekingen in de vitale nationale infrastructuur voor de goede werking van de economie onder de aandacht van het Witte Huis.

50 United States of America government, Department of Commerce, National Institute of Standards and Technology. Cybersecurity framework. NIST, online (geraadpleegd op 16/02/2018). Zie https://www.nist.gov/cyberframework

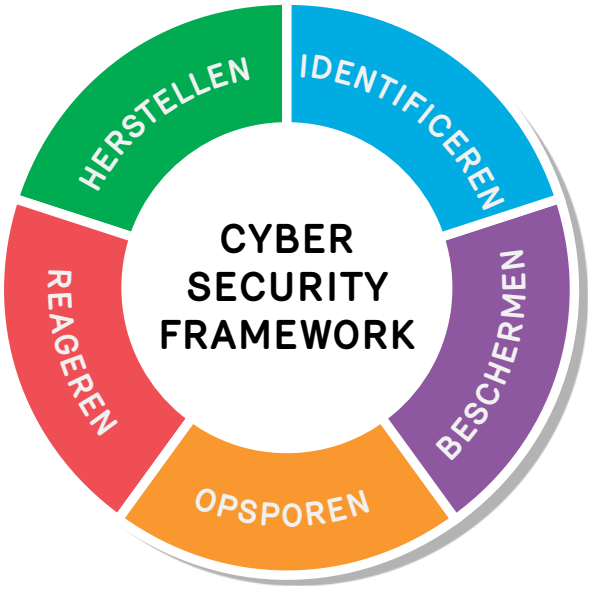
Bij het ontstaan van het CSF in 2014 werd het methodologische kader door consultancybureau PriceWaterhouseCoopers al beschouwd als *"een kantelpunt in de evolutie van cyberveiligheid, waarbij het zwaartepunt verschuift van reactieve naleving naar proactieve risicobeheerstandaarden"*. [51] Volgens het bureau Gartner zal de helft van de openbare en privéorganisaties tegen 2020 CSF gebruiken [52].

De 5 basisfuncties van een cyberveiligheidsplan

Het CSF onderscheidt zich door zijn globale kijk op de problematiek en door zijn links met andere normen en referenties. Het geeft beheerders of technici de mogelijkheid om via verschillende bronnen alle nodige technische gegevens te verzamelen voor de implementering van de aanbevolen maatregelen.

Het CSF, herzien in 2017, definieert de vijf basisfuncties van een cyberveiligheidsplan: identificeren, beschermen, opsporen, reageren en herstellen.

- **Identificeren:** organisatorisch inzicht ontwikkelen om een correct beeld te schetsen van het cyberrisico voor de systemen, mensen, middelen, gegevens en capaciteiten van de organisatie
- **Beschermen:** passende waarborgen ontwikkelen en implementeren om een ononderbroken dienstverlening van kritieke infrastructuren te garanderen
- **Opsporen:** passende acties ontwikkelen en implementeren om gebeurtenissen op te sporen die de cyberveiligheid in het gedrang brengen wanneer deze zich voordoen
- **Reageren:** de nodige acties ontwikkelen en implementeren om te reageren op de gebeurtenissen die de cyberveiligheid in het gedrang brengen
- **Herstellen:** de nodige acties ontwikkelen en implementeren om de plannen om de veerkracht up-to-date te houden en de door een cyberincident getroffen diensten en/of infrastructuren te herstellen



51 PriceWaterhouseCoopers, Why you should adopt the NIST Cybersecurity Framework. 2014. Online (geraadpleegd op 16/02/2018). Zie http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

52 United States of America government, Department of Commerce, National Institute of Standards and Technology. Cybersecurity «Rosetta Stone» Celebrates Two Years of Success. News, NIST, 18 februari 2016, online (geraadpleegd op 16/02/2018). Zie https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success

4.2. De 2700x-normen van de Internationale Organisatie voor Standaardisatie (ISO).

De normenfamilie ISO/IEC 2700x is van toepassing op beheersystemen voor informatieveiligheid. Het doelpubliek omvat alle mogelijke types organisaties, ongeacht hun omvang, van privébedrijven tot vzw's en openbare diensten.

De ISO 2700x-normen zijn samengebracht onder de noemer "Beveiligingstechnieken voor informatietechnologie" en helpen organisaties in de strijd tegen uiteenlopende en zich steeds sneller uitbreidende vormen van cyberdreiging. Alle cyberveiligheidstoepassingen zijn erin opgenomen. Het gaat in totaal om meer dan een dozijn normen die elk op hun niveau gekoppeld zijn aan de middelen en methoden die moeten worden ingezet om zich te beveiligen tegen of het hoofd te bieden aan de gevaren in de ICT-omgeving.

De toepassingsgebieden van de ISO 2700x-normen omvatten incidentenbeheer, waaronder rampenplannen, systeemonderbrekingen, verstoring van de activiteiten en malwareaanvallen door bijvoorbeeld virussen, wormen en Trojaanse paarden. De normen liggen trouwens aan de basis van beveiligingskenmerken die worden toegepast in tal van producten, technologieën en softwaretoepassingen. Ze vormen dus een oplossingenpakket waarmee organisaties hun kritieke en gevoelige informatie en persoonsgegevens kunnen beschermen, ongeacht de economische sector waartoe ze behoren of de organisatorische structuur.

De vereisten voor beheersystemen inzake informatiebeveiliging zitten vooral vervat in de ISO 27001-norm, die praktijken beschrijft voor optimaal risicobeheer. Het doel is om een antwoord te bieden op problemen inzake beveiliging, vertrouwelijkheid en risico-evaluatie en -beheer.

Langetermijnvisie en basis voor vertrouwen

Net zoals het CSF omvat ISO 27001 een methodologie voor een georganiseerde, operationele cyberbeveiliging. Deze norm past in elk implementatie- en ontwikkelingsstadium van de cyberveiligheidsmaatregelen het Plan, Do, Check, Act-principe toe. Bijgevolg onderscheidt ze zich door de grotere nadruk die gelegd wordt op de nood aan langetermijnacties. Zoals bij elke ISO-norm zijn er bovendien certificeringsprocessen aan verbonden voor de personeelsleden die met deze vraagstukken belast worden. Die processen vormen de basis van het wederzijdse vertrouwen tussen actoren in hun vermogen om te gaan met cyberveiligheidsvraagstukken.

Ook het CIBG en de betrokken medewerkers passen de door de ISO 2700x-normen vastgelegde methodologieën toe, met name in het kader van de eigen strategische diensten en infrastructuren, zoals het Gewestelijk Data Center, en ook in het aan de partners voorgestelde aanbod inzake Information Security Management. Dat aanbod richt zich specifiek tot organisaties die toegang wensen tot vertrouwelijke gegevens (authentieke bronnen) en in dat kader door de Europese, federale en gewestelijke overheden bepaalde veiligheidseisen opgelegd krijgen. Het CIBG suggereert daartoe de invoering van een strategisch veiligheidsplan dat voldoet aan de beste praktijken van de internationale ISO 2700x-norm. Dat plan omvat technische beveiligingsmaatregelen en processen die nodig zijn om te voldoen aan de wetten en normen die worden opgelegd door organisaties zoals het Rijksregister (RRN), de Kruispuntbank van de Sociale Zekerheid (KSZ), enz.

3.

EEN CYBERVEILIGHEIDSPLAN VOOR HET BRUSSELS HOOFDSTEDELIJK GEWEST

Een cyberveiligheidsplan voor het Brussels Hoofdstedelijk Gewest moet de operationele capaciteit van de informaticasystemen en -infrastructuren van het gewest en in het bijzonder zijn kritieke infrastructuren beschermen tegen cyberaanvallen. Het veronderstelt ook dat de algemene evolutie van cyberdreigingen wordt opgevolgd en dat het gewestelijk reactievermogen wordt georganiseerd voor een optimale veerkracht. Het gewest moet daartoe alle nodige middelen inzetten met het oog op de na te leven regels en de audits en voor het delen van beste praktijken en aanbevelingen die in de breedst mogelijke zin moeten worden gedeeld en geïmplementeerd in samenwerking met alle bevoegde autoriteiten.

1. 4 KRACHTLIJNEN: CYBERVEERKRACHT, RESOURCES, CULTUUR EN PREVENTIE

Het cyberveiligheidsplan van het Brussels Hoofdstedelijk Gewest moet uiteenlopende doelgroepen ertoe aanzetten om de principes ervan om te zetten in adequaat gedrag.

Samengevat bestaat de strategie uit de 4 krachtlijnen en richt zich tot 4 doelgroepen:

4 KRACHTLIJNEN	4 DOELGROEPEN
• de cyberveerkracht van de kritieke infrastructuren organiseren • de industriële, technologische en menselijke resources ontwikkelen • mensen bewustmaken en laten kennismaken met een cyberveiligheidscultuur • cyberincidenten voorkomen en de samenwerking met de bevoegde actoren inzake cyberbeveiliging en cybercriminaliteit opvoeren	• openbare diensten • bedrijven • de academische wereld • de burger

1.1. De cyberveerkracht van de kritieke infrastructuren organiseren

Om de cyberveerkracht van ons gewest te organiseren, moeten we ten eerste potentiële doelwitten identificeren. In het eerste hoofdstuk zagen we hoe verscheiden zowel de aanvalsmogelijkheden als de doelwitten zijn. Wanneer we een lijst willen opstellen met kritieke infrastructuren van het Brussels Hoofdstedelijk Gewest, moeten we daarom een zo breed mogelijke blik hanteren.

De eerste krachtlijn van de strategie moet een antwoord bieden op enkele cruciale vragen: wat is een kritieke infrastructuur, wat zijn de voorbeelden daarvan in het Gewest, waarom moeten die infrastructuren beschermd worden en welke rol moet het gewest daarin spelen?

<u>De rol van het CIBG en BPV in de aanpassing van de NIS-richtlijn</u>

De stappen op dit niveau moeten worden ingepast in het door de federale overheid aangereikte kader voor de aanpassing van de NIS-richtlijn conform het Belgische recht [1]. Het CCB, dat met de reflectie over die omzetting is belast, heeft met name voorgesteld om de overheidssector op te nemen in de lijst van aanbieders van essentiële diensten (AED's) om een beroep te doen op sectorale overheden en om de gewestoverheden te raadplegen.

1 Zie hoger: kaderstuk "De NIS-richtlijn in België", pagina's 28 en 29.

Voor deze drie aspecten beschouwen het CIBG en BPV zich als natuurlijke aanspreekpunten en vertegenwoordigers van het Brussels Hoofdstedelijk Gewest voor het CCB voor het vervullen van deze opdracht.

De Brusselse Regering wil ook dat er bijzondere aandacht wordt besteed aan deze materie. Daarom heeft de regering de GVPP-maatregel goedgekeurd voor "*de oprichting van een technologische controlegroep die bestaat uit specialisten die de opdracht krijgen om technische en technologische innovaties te identificeren met een meerwaarde op het vlak van crisisbeheer en veerkracht*". [2]

A. Opstellen en bijwerken van een gewestelijke studie inzake de cyberveiligheidsrisico's

Als we aannemen dat kennis macht is, zoals het spreekwoord het wil, dan vormt kennis de basis van een degelijk cyberveiligheidsplan. Die kennis moet worden gecentraliseerd en gedeeld. In dat opzicht is het nuttig om een register aan te leggen van risico's op gewestniveau en ervoor te zorgen dat het regelmatig wordt bijgewerkt afhankelijk van de evolutie van de infrastructuren enerzijds en van de dreigingen en kwetsbare punten anderzijds. Het identificeren van kritieke infrastructuren is de eerste taak.

Wat is een kritieke infrastructuur?

Wanneer we denken aan de infrastructuren waarvan de verstoring in geval van een cyberaanval risico's inhoudt voor de continuïteit van essentiële diensten, denken we meteen aan enkele logische voorbeelden: vervoersnetten, productie en distributie van water en energie, veiligheid, gezondheid...

Als basiskader voor een anti-cybercriminaliteitsbeleid voor alle EU-lidstaten is de NIS-richtlijn ook betekenisvol voor het Brussels Hoofdstedelijk Gewest. In het kader van het cyberveiligheidsplan moet het gewest fungeren als contactpunt voor het CCB (federaal niveau) voor de implementatie van de NIS-richtlijn [3] op het grondgebied met de volgende twee doelen:

- de eventuele aanpassing van de gewestwetgeving
- de identificatie op het terrein van de kritieke gewestinfrastructuren

Bepaalde door de Brusselse openbare besturen beheerde infrastructuren vallen rechtstreeks onder de NIS-richtlijn [4] omdat ze behoren tot een van de onderstaande in de richtlijn opgesomde sectoren:

- distributienetwerkbeheerders en transmissienetbeheerders voor aardgas en elektriciteit;
- havenbeheerders
- wegenautoriteiten voor verkeerscontrole en -beheer en exploitanten van intelligente transportsystemen
- kredietinstellingen
- leveranciers en distributeurs van water bestemd voor menselijke consumptie
- IXP's, leveranciers van DNS-diensten, registers van domeinnamen van hoog niveau

2 Globaal veiligheids- en preventieplan. Zie hoger. Pagina 49, maatregel 10.13.
3 Zie hoger op pagina 26.
4 Zie de lijst van de door de NIS-richtlijn opgesomde sectoren en subsectoren, pagina 27.

Bij het opstellen van de inventaris van kritieke gewestinfrastructuren kan nuttig gebruik worden gemaakt van definities die worden aangereikt door verschillende EU-lidstaten. Zo heeft men in Frankrijk het concept van de 'opérateur d'importance vitale' (OIV, operator van vitaal belang) ingevoerd. De definitie van OIV is breder en omvat:

- overheids- en privé-exploitanten die vestigingen uitbaten of installaties gebruiken waarvan de uitval een aanzienlijke vermindering met zich mee dreigt te brengen van het militair of economisch potentieel of van de veiligheid of de overlevingskansen van de natie
- bepaalde vestigingen waaraan een gevaar voor het milieu verbonden is of die een nucleaire installatie behelzen

Globale kijk op de risico's

De geweststudie inzake de cyberveiligheidsrisico's moet trouwens ook rekening houden met bepaalde factoren die de schade potentieel kunnen verergeren, zoals:

- onderlinge afhankelijkheid tussen informaticasystemen die leidt tot het risico op een totale ineenstorting door een domino-effect
- geërfde, oudere informaticasystemen waardoor het afslaan van een aanval vertraging kan oplopen, bijvoorbeeld omdat er geen documentatie voor de systemen meer voorhanden is of de leverancier niet meer bestaat of de systemen niet meer ondersteunt: dit aandachtspunt is opgenomen in de cyberveiligheidsstrategieën in Nederland en het Verenigd Koninkrijk [5]
- de verspreiding van verbonden voorwerpen in de omgeving, zowel thuis (bijv. domotica-oplossingen) als in de publieke ruimte (waarvoor momenteel intelligente uitrusting wordt ontwikkeld in het kader van de Smart City)

HOE IS DE CYBERVEERKRACHT GEORGANISEERD, IN WELKE MATE, DOOR WELKE ACTOREN?

Bovendien moet men in de inventaris ook de geïmplementeerde maatregelen opnemen: hoe is de cyberveerkracht georganiseerd, in welke mate, door welke actoren, volgens welke regels en procedures, hoe duurzaam is dat alles...?

B. Een gewestelijk register van sleutelpersonen opstellen

De doeltreffendheid van een actieplan inzake cyberveiligheid wat zowel theoretische uitwerking als aanpassing en uitvoering betreft, berust niet alleen op een correcte risicobepaling, maar ook op de identificatie van de personen wier functie en handelen binnen hun organisatie doorslaggevend zijn in geval van een grootschalige crisis.

Daarvoor moet het gewestelijk cyberveiligheidsregister dienen. Daarin tekenen alle beheerders van een kritieke infrastructuur de contactgegevens op van de betrokken veiligheidsverantwoordelijke. Dat register moet op een beveiligde manier worden gedeeld onder de betrokken beheerders en moet vanzelfsprekend constant worden bijgewerkt.

Een van de maatregelen van het GVPP [6] betreft de aanleg van dit register, dat de gewestelijke preventie- en veiligheidsactoren bewust moet maken "van het belang van het aanduiden

5 United Kingdom, Cabinet Office. National Cyber Security Strategy 2016 to 2021. Policy paper. Publications, UK government, 1 november 2016, online (geraadpleegd op 16/02/2018). Zie https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

6 Globaal veiligheids- en preventieplan. Zie hoger. Pagina 43, maatregel 8.12

van een IT-contactpunt bij elke gewestelijke, zonale en gemeentelijke administratie om de informatie die het Centrum voor Cybersecurity België (CCB) verspreidt, door te geven."

Dat register moet overigens helpen bij het opbouwen van een cyberveiligheidsgemeenschap binnen het Brussels Hoofdstedelijk Gewest, als platform voor het bundelen van middelen en nuttige informatie.

C. Minimale veiligheidsvereisten vastleggen per sector

Zoals eerder reeds aangehaald, zijn bepaalde bepalingen van de NIS-richtlijn rechtstreeks van toepassing op sommige Brusselse aanbieders (openbare of privéoperatoren of entiteiten die actief zijn binnen een publiek-privépartnerschap). Ze kunnen ook als referentie dienen voor sectoren of aanbieders die de richtlijn niet rechtstreeks beoogt. Bovendien moet ook rekening worden gehouden met de regels en aanbevelingen vanaf Belgisch federaal niveau.

Wij pleiten voor het bepalen van een minimaal beveiligingsniveau per sector op basis van de Europese of nationale normen ter harmonisering van de aanpak, verspreiding van beste praktijken en bepaling van prioriteiten op het vlak van toekomstige investeringen.

D. Een label voor kritieke infrastructuren

Een gewestlabel voor cyberbeveiliging zal het plan zichtbaarder maken, waardoor het zijn doel ook beter zal bereiken. Een label wekt vertrouwen bij de gebruikers van diensten en vertrouwen vormt volgens de Europese Unie de hoeksteen van de digitale eengemaakte markt. Zo'n label zou aanduiden welke publieke instanties, bedrijven en handelszaken hun verplichtingen naleven en goede praktijken hanteren om zich te beschermen tegen cyberincidenten.

Deze stap moet in het verlengde liggen van initiatieven van het CCB in het kader van de aanpassing van de NIS-richtlijn conform het Belgische recht. Ook hier heeft de Brusselse Regering goedkeuring gegeven in het kader van het GVPP, maatregel 8.11 [7] "Voor bedrijven algemene gedragsregels inzake veiligheid opstellen; een gewestelijk beleid in die zin uitwerken en een gewestelijk label afleveren (IT- veiligheidscertificaat) aan bedrijven die zich hierop toeleggen".

E. De implementatie van de minimale veiligheidsvereisten per sector bevorderen

Niet alleen een label, maar ook het ondersteunen van de organisaties bij hun inspanningen om de risico's te identificeren, zich ertegen te beschermen en ervoor te zorgen dat ze over de middelen beschikken om op incidenten te reageren is een stimulans om het gewestelijke cyberveiligheidsplan te hanteren.

Daarom bevelen we aan om de betrokken actoren hulpmiddelen aan te bieden voor de implementatie van de cyberveiligheidsrichtlijnen en -normen, waaronder met name een model van een noodplan per sector met aanduiding van de incidentniveaus, verantwoordelijken en voorbeeldacties.

F. Een gewestelijk CERT oprichten

Het federaal Cyber Emergency Team, CERT.be, is belast met de CERT-activiteiten op het niveau van de Belgische federale regering. Het team heeft een dubbele opdracht: enerzijds de coördinatie van de aanpak en het beantwoorden van incidenten ('incident handling

7 Globaal veiligheids- en preventieplan. Zie hoger. Pagina 43, maatregel 11

and response') in geval van nationale incidenten en crisissituaties bij exploitanten van kritieke infrastructuren of aanbieders van essentiële diensten, en anderzijds fungeren als informatiebron.

De diensten van het team zijn echter niet beschikbaar voor de gewestelijke actoren en bedrijven tenzij in geval van een nationale crisis. Er is een gewestelijk Cyber Emergency Team nodig om hulp te bieden aan privébedrijven en overheidsinstanties wanneer zij op hun niveau te maken krijgen met een ernstig incident. De werkzaamheden van dit gewestelijk CERT zouden worden georganiseerd in overleg met het federale team.

G. Een gewestelijk cybernoodplan opstellen

Als aanvulling op de identificatie en het beheer van risico's (cf. punt A hieboven) moeten verschillende scenario's voor de continuïteit en de daaropvolgende normale hervatting van de activiteiten worden opgesteld om het hoofd te bieden aan potentiële cybercrises.

In samenloop met het nationale plan moet het gewestelijk cybernoodplan de volgende elementen vastleggen:

- de criteria van wat precies een crisis is op de schaal van het Brussels Hoofdstedelijk Gewest
- de belangrijkste processen en acties die nodig zijn om zo'n crisis te beheren
- de rollen en verantwoordelijkheden van de belangrijkste actoren tijdens een crisis

H. Cyberveiligheidsoefeningen organiseren

Hierbij is het de bedoeling te evalueren in welke mate de belangrijkste actoren gewapend zijn tegen een cyberaanval. Daarbij gaat het erom de noodplannen te testen om zicht te krijgen op onderlinge afhankelijkheidsrelaties en zwakke punten waarmee geen of te weinig rekening is gehouden, en de samenwerking tussen de verschillende sectoren te verbeteren.

Zulke oefeningen kunnen zich initieel beperken tot de informaticadiensten van de besturen, vervolgens tot de besturen zelf en daarna nog verder worden uitgebreid.

1.2. De industriële, technologische en menselijke resources ontwikkelen

Om zich te beschermen tegen cyberrisico's moet men een beroep kunnen doen op diverse resources. Dat wil zeggen de beschikbare producten en diensten aanwenden én ervoor zorgen dat men beschikt over de nodige kennis en competenties om gegevens en infrastructuren te beschermen.

Maar, zoals Evoliris vaststelde in zijn observatierapport 2017 'Schijnwerper op de Cyberveiligheid in Brussel' [8], hebben we vandaag te maken met een "*gebrek aan opleidingen in Cyberveiligheid [...] Het is belangrijk dat de onderwijsinstellingen en de ondernemingen hiervoor samen aan tafel zitten. En dat wordt voornamelijk de rol van de PFE (Frans voor Pôle Formation Emploi): de Opleidings- en tewerkstellingspool voor ICT [die] is voorzien tegen eind 2018.*" Een van de PFE's taken is mensen warm maken voor IT-beroepen, dus wordt de organisatie zonder enige twijfel een onmisbare speler in het toekomstige gewestelijke cyberveiligheidsplan.

8 Evoliris. Schijnwerper op de Cyberveiligheid in Brussel. Evoliris zoomt in op ..., nr. 2, 2017, online (geraadpleegd op 01/06/2018). Zie http://www.evoliris.be/nl/content/schijnwerper-op-de-cyberveiligheid-brussel-de-sensibilisering-voorbij

Het plan zal op dat vlak tot doel hebben in het Brussels Hoofdstedelijk Gewest een ecosysteem van cyberveiligheid tot stand te brengen, met als belangrijkste spelers de bedrijven uit de ICT-sector en onderwijskringen, waaronder de Gewestelijke School voor Veiligheidsberoepen.

A. Bedrijven in de cyberveiligheidssector aanmoedigen

De diverse, voortdurend in kracht toenemende vormen van cyberdreiging bieden groeikansen voor de Brusselse ICT-sector, die zijn diensten kan aanbieden aan bedrijven en overheidsinstanties. Het gewestelijk cyberveiligheidsplan moet de gewestelijke ICT-bedrijven aanmoedigen om hun ontwikkeling in dat domein toe te spitsen.

Die beweging kan nuttig en doeltreffend afgestemd worden met verschillende gesprekspartners, zoals de sectorfederatie AGORIA, de bedrijvenclusters en de academische en onderzoekskringen. Om hier concreet vorm aan te geven, kan bijvoorbeeld gedacht worden aan de creatie van bepaalde hulpmiddelen, zoals een handvest, om de sector te organiseren en te promoten.

Op die manier kan het cyberveiligheidsplan het Brussels Hoofdstedelijk Gewest en zijn ICT-sector helpen een imago op te bouwen dat in het teken staat van uitmuntendheid en innovatie.

B. Uitwisseling op academisch en onderzoeksvlak stimuleren

Een gewest dat zich wil beschermen tegen cyberrisico's moet zijn kenniseconomie ontwikkelen en dus in de eerste plaats kwaliteitsonderwijs in dat domein ondersteunen en onderzoek van het hoogste niveau stimuleren.

Het Brussels Hoofdstedelijk Gewest doet er goed aan om zich op te werpen als kenniscentrum, om te beginnen door een inventaris op te stellen van de onderwijs- en onderzoekscentra die een band hebben met cyberveiligheid, om die spelers aan te zetten tot samenwerking en uitwisseling, bijvoorbeeld in het kader van gemeenschappelijke en/of welomlijnde projecten.

Een groot deel van die inventarisering heeft Evoliris al gerealiseerd in zijn 'Schijnwerper op de Cyberveiligheid in Brussel' dat een overzicht biedt van de opleidingen die worden aangeboden in het Brussels hoger onderwijs (door zowel de universiteiten als de hogescholen) en in het kader van certificeringstrajecten en permanente educatie.

Het gewest kan hiervoor in het kader van het plan ondersteuning bieden door geld, beurzen enz. ter beschikking te stellen.

C. Onderzoek naar en ontwikkeling van cyberbeveiligingsproducten en -diensten ondersteunen

Als aanvulling op het voorgaande moet het gewestelijk cyberveiligheidsplan het gemakkelijker maken om wetenschappelijke en/of technische kennis voor concrete toepassingen in te zetten.

Hier moet op twee manieren aan gewerkt worden:

- het ter beschikking stellen van overheidsgeld voor de ondersteuning van onderzoek en ontwikkeling, met name door startups of spin-offs
- het creëren van promotietools en stimulansen voor bedrijven om hun zichtbaarheid te verhogen, onderzoek te promoten en producten of diensten te commercialiseren

D. Basisbehoeften inzake beveiligingsproducten en -diensten dekken

Het is van essentieel belang dat burgers, bedrijven en openbare besturen beschikken over een arsenaal van cyberbeveiligingstools afgestemd op hun behoeften en gebruikswijzen. Als de risico's waaraan ze blootstaan niet volledig kunnen worden afgedekt door de op de markt beschikbare producten en diensten, moet er voor oplossingen worden gezorgd.

E. De ontwikkeling van academische curricula aanmoedigen

Het Brussels Hoofdstedelijk Gewest, zijn bedrijven en openbare besturen hebben mensen nodig die zijn opgeleid in de verschillende aspecten van cyberveiligheid. Die cyberveiligheid houdt niet enkel verband met informatica, maar ook met telecommunicatienetwerken (met name de mobiele) en geconnecteerde voorwerpen.

Het is de taak van het onderwijs (vooral het hoger onderwijs) om voor al die aspecten opleidingen te voorzien. In het strategische belang van het gewest zal het gewestelijk cyberveiligheidsplan een inventaris opstellen van de opleidingen die verband houden met cyberveiligheid, en hun inhoud, reikwijdte (bereikt publiek) en coherentie analyseren. Indien nodig zullen specifieke acties worden ondernomen om bepaalde opleidingen te promoten.

HET IS VAN ESSENTIEEL BELANG DAT BURGERS, BEDRIJVEN EN OPENBARE BESTUREN BESCHIKKEN OVER EEN ARSENAAL VAN CYBERBEVEILIGINGSTOOLS

<u>Geïntegreerde school voor veiligheids-, preventie- en hulpverleningsberoepen</u>

In haar **strategische nota** met betrekking tot de uitoefening van de Brusselse gewestelijke bevoegdheden inzake preventie en veiligheid van 28/4/2016 besloot de Brusselse Regering om een Geïntegreerde School voor Veiligheids-, preventie- en hulpverleningsberoepen op te richten (kortweg Gewestelijke School voor Veiligheidsberoepen, GSVB).

De taken van de GSVB zijn onder meer:

- een geïntegreerde en multidisciplinaire visie op de openbare veiligheid in de brede zin in de praktijk brengen;
- de scholen steunen die betrokken zijn bij de opleiding van preventie- en veiligheidsactoren door de gemeenschappelijke benutting van gemeenschappelijke processen (zoals een pedagogische cel, ICT-ondersteuning, logistiek enz.);
- de scholen ondersteunen door een gemeenschappelijke en multidisciplinaire infrastructuur ter beschikking te stellen waarmee de cursisten kunnen worden opgevangen en voor ieder vakgebied geïntegreerde en/of specifieke oefeningen kunnen worden georganiseerd;
- de bestaande kennis en infrastructuur ter beschikking stellen van openbare en zelfs privéorganisaties voor zover hun activiteiten beantwoorden aan de opdrachten van de school.

Met de door het GVPP [9] naar voren geschoven visie als inspiratie zal de GSVB naast een regionaal overzicht van de scholen en de beschikbare cursussen ook het volgende aanbieden:

- nieuwe leer- en informatietechnologieën, die het werken in een netwerk bevorderen, en de beveiliging van de digitale hulpmiddelen en het internetgebruik;
- op het gebied van crisisbeheersing en weerbaarheid: aanvullend op de organisatie van regelmatige gezamenlijke oefeningen op basis van reële scenario's voor veiligheids- en reddingsactoren, het personeel opleiden in het gebruik van communicatiemiddelen (Astrid, digitaal platform) en crisisbeheersing.

Met het oog op de omzetting van de intentie van de Brusselse Regering zal een van de hoofdopdrachten van de GSVB zijn om de specialisatie op het gebied van opleiding te versterken, de bestaande partnerships te integreren en nieuwe akkoorden te ontwikkelen. In dit opzicht zullen er samenwerkingsverbanden met universiteiten worden tot stand gebracht, met name in het kader van specifieke opleidingen (bijvoorbeeld inzake cybercriminaliteit of computerbeveiliging).

F. Toegang tot opleidingen aanmoedigen en vergemakkelijken

Ook voor trajecten voor levenslang leren is er een rol weggelegd in de verspreiding van competenties en de verhoging van de waakzaamheid op het vlak van cyberveiligheid, zowel in huiselijke als professionele kring.

Specifiek kunnen opleidingsstimulansen in het leven worden geroepen om zelfstandigen, kmo's en grote bedrijven te helpen hun cyberbeveiliging te verbeteren.

1.3. Een cyberveiligheidscultuur bevorderen

Een bloeiende economie steunt op het vertrouwen van bedrijven en burgers in de onlinediensten. Het behoort tot de taak van de overheid om te zorgen voor de bewustmaking van alle actoren, om te komen tot verantwoordelijk gedrag zodat grote en kleine bedrijven en ook burgers zichzelf en degenen voor wie ze verantwoordelijk zijn (bijvoorbeeld hun klanten in het geval van bedrijven of hun kinderen in het geval van burgers) adequaat beschermen.

A. Zelfstandigen, ambachtslui en bedrijven sensibiliseren

De economie en werkgelegenheid in het Brussels Hoofdstedelijk Gewest steunen voor een groot deel op de werkzaamheden van een enorm aantal zelfstandigen, ambachtslui, kmo's en een zeer kleine ondernemingen (ZKO's) die ongeacht hun omvang of bedrijfstak onvermijdelijk ICT inzetten als hulpmiddel bij hun beroepsbezigheden (boekhoudkundige en vakspecifieke software, websites, onlinewinkels).

Het is dan ook van het grootste belang dat het Brussels Hoofdstedelijk Gewest deze voor zijn welvaart cruciale actoren helpt zich te beschermen tegen cyberrisico's en ze het hoofd te bieden. Dat is nodig om zowel hun activiteiten als het vertrouwen van derden in die activiteiten te bestendigen.

Daarom moet het cyberveiligheidsplan voorzien in de organisatie van communicatie- en sensibiliseringscampagnes of het verlenen van medewerking daaraan in het kader

9 Globaal veiligheids- en preventieplan. Zie hoger. Overkoepelende doelstellingen - De opleiding van preventie- en veiligheidsactoren. Pagina 7 en 8

van deze strategische doelstelling voor het Gewest. Het valt dan ook aan te bevelen dat de relevante gewestelijke cyberveiligheids- en economische actoren op zoek gaan naar partnerships met belangrijke vertegenwoordigers van deze doelgroepen, zoals bijvoorbeeld de sectorfederaties.

B. Het invoeren van beste praktijken door zelfstandigen en bedrijven aanmoedigen

Als aanvulling op de sensibilisering voor niet te onderschatten cyberrisico's moet men zelfstandigen en bedrijven aanmoedigen om goede praktijken inzake cyberveiligheid in te voeren, desgevallend ook in het kader van hun verplichtingen op dat vlak.

Daartoe kan het Brussels Hoofdstedelijk Gewest op eigen initiatief of in samenwerking met anderen bijvoorbeeld:

- de toegang tot die beste praktijken vereenvoudigen;
- helpen om die beste praktijken toe te passen;
- erop toezien dat informatie afkomstig van andere instanties (zoals het CCB of het ENISA) hen tijdig bereikt.

Naast de traditionele communicatiekanalen kan het Brussels Hoofdstedelijk Gewest gebruikmaken van de hulpmiddelen die het geschiktst zijn voor de verspreiding van beste praktijken. Een Brussels handvest voor cyberveiligheid en ethisch verantwoorde omgang met persoonsgegevens kan bijvoorbeeld dienen als herkenningspunt dat het vertrouwen van klanten in zelfstandigen, ambachtslui en bedrijven stimuleert.

C. Bij de economische actoren de juiste reflexen stimuleren voor het geval zich een incident voordoet

Tegelijk met de verspreiding van beste praktijken onder zelfstandigen, ambachtslui en kmo's moet het Brussels Hoofdstedelijk Gewest hen helpen om de juiste reflexen aan te leren in geval van incidenten. In navolging van op het grote publiek gerichte campagnes om de mensen te vertellen welk nummer ze moeten draaien om de politie of de brandweer te bellen, moet het cyberveiligheidsplan ervoor zorgen dat iedereen weet waar hij terechtkan in geval van een cyberincident. Een van de taken van het gewestelijk CERT is om in die context te fungeren als contactpunt.

D. De burger sensibiliseren

Het grote publiek is een volwaardige doelgroep voor promotiecampagnes rond cyberveiligheid, want het is zelf vaak slachtoffer en/of doorgeefluik van cyberaanvallen. Het is de taak van het cyberveiligheidsplan om de burger bewust te maken van en waakzaam te maken voor cyberrisico's, zowel via specifieke eigen acties als door medewerking aan acties van anderen. Zulke acties maken het voorwerp uit van maatregel 8.11 van het GVPP die adviseert een campagne te ontwikkelen om het publiek bewust te maken van cyberveiligheid [10].

E. De burger aanzetten om goede gewoonten aan te nemen

De burgers moeten zelf actief bezig zijn met hun cyberveiligheid. Ze moeten dan ook op de hoogte zijn van de beste praktijken, waaronder bepaalde basisreflexen in hun dagelijkse ICT-gebruik. Heel wat actoren zetten zich al in voor de verspreiding van beste praktijken op dit vlak. De rol van het Brussels Hoofdstedelijk Gewest is om te helpen bij de verspreiding van die informatie en de omzetting ervan in de praktijk te onderzoeken. In

10 Globaal veiligheids- en preventieplan. Zie hoger. Pagina 43, maatregel 11

rechtstreeks verband met het beleid voor het dichten van de digitale kloof gaat het Brussels Hoofdstedelijk Gewest er met name op toezien dat iedereen niet alleen toegang heeft tot ICT en de mogelijkheden van het internet maar daar ook veilig (zowel voor zichzelf als voor anderen) gebruik van maakt.

F. Bij de burger de juiste reflexen stimuleren voor het geval zich een incident voordoet

Net als bedrijven moet burgers weten waar ze terechtkunnen wanneer ze worden getroffen door een cyberaanval om eventuele schade te beperken, de aanval in te dijken en cybercriminelen makkelijker op te sporen en te vervolgen. Het gewestelijk cyberveiligheidsplan moet dan ook noodadressen verspreiden in samenwerking met andere instanties.

1.4. Cyberincidenten voorkomen

In samenloop met de evolutie van nieuwe technologieën werd op het vlak van criminaliteit de afgelopen jaren een belangrijke verschuiving van de ontwikkeling van criminele activiteiten vastgesteld van de openbare naar de virtuele ruimte. Cybercriminaliteit maakt tegenwoordig integraal deel uit van de risico's van het dagelijks leven en vereist toegenomen aandacht van de autoriteiten. Er is derhalve nood aan grote investeringen in de ontwikkeling van nieuwe onderzoeks- en actiemiddelen.

In haar GVPP heeft de Brusselse Regering al blijk gegeven van de intentie om van de strijd tegen cybercriminaliteit een van de tien prioritaire thema's voor de komende jaren te maken. In lijn met de globale strategie van het GVPP worden verschillende maatregelen voorzien om "de *opsporingsactiviteiten op het darknet te versterken om de ontwikkeling van verscheidene misdaadfenomenen (drughandel, wapenhandel, preventie van en strijd tegen terrorisme en radicalisering) proactief te bestrijden en de informatie-uitwisseling die eruit voortkomt tussen de bevoegde diensten te bevorderen*" [11] (M8.14).

A. Voorkomen dat potentiële toekomstige cybercriminelen tot de daad overgaan

Met het oog op de voortzetting van de aanpak van het GVPP zal een 'gewestelijk cyberveiligheidscentrum' worden opgericht.

De relevantie van zo'n hulpmiddel is al verschillende keren aangetoond nu nieuwe communicatiekanalen ook worden gebruikt om oproepen tot samenkomsten en geweld te lanceren. Toegenomen waakzaamheid vanwege de bestuurlijke en gerechtelijke autoriteiten is dan ook onmisbaar geworden, vooral wat betreft het in de gaten houden van de activiteit op de sociale media.

Het Gewestelijk cyberveiligheidscentrum zal werken met vertegenwoordigers van de Regional Computer Crime Unit van de federale gerechtelijke politie, de zes plaatselijke politiezones van het gewest en de directie coördinatie van de federale politie. Die samenwerking zal verlopen op basis van een overeenkomst waarin de modaliteiten van de samenwerking tussen de entiteiten worden vastgelegd.

De oprichting van een technische controlegroep zal helpen de gewestelijke doelstellingen te versterken en te concretiseren. Die controlegroep zal gebruik kunnen maken van de gedeelde technische hulpmiddelen, waaronder observatiesoftware aangekocht door het Brussels Hoofdstedelijk Gewest. Het doel hiervan is te voorkomen dat Brusselaars worden

11 Globaal veiligheids- en preventieplan. Zie hoger. Pagina 43, maatregel 8.14

ingeschakeld in cybercriminaliteitsnetwerken. Het cyberveiligheidsplan voorziet daartoe in:

- acties binnen het onderwijs en specifiek gericht op het publiek van informaticacursussen (in het middelbaar en hoger onderwijs), via getuigenissen van politiemensen, tot inkeer gekomen criminelen enz.;
- ontrading via de versterking van de ICT-infrastructuren in het gewest en met name via de bescherming van kritieke infrastructuren.

Het gewestelijk CERT zal helpen om het risico op cyberincidenten op het grondgebied van het gewest te voorkomen en te beperken, maar ook ondersteuning bieden mochten deze zich voordoen.

B. Onderzoeksvaardigheden versterken

Door de zeer specifieke technieken moet men in de strijd tegen cybercriminaliteit een beroep kunnen doen op specialisten wat zowel theoretische – en juridische - kennis – betreft als de praktijk. Via het gewestelijke cyberveiligheidsplan zal er op zoek worden gegaan naar manieren om de opleiding van de betrokkenen te ondersteunen om snel en doeltreffend de technieken van cybercriminelen te identificeren of in de cyberspace van cybercriminaliteitsnetwerken te infiltreren om hun activiteiten te bestrijden. Er moet worden voorzien in opleidingsmogelijkheden op het vlak van cybercriminologie en in de mogelijkheid om een beroep te doen op ethische hackers.

Dit zal in de eerste plaats gebeuren in het kader van de ontwikkeling van nieuwe opleidingen in samenwerking met de Gewestelijke School voor Veiligheidsberoepen en de onderwijssector.

C. Samenwerken op federaal en internationaal niveau

De actoren van het cyberveiligheidsplan moeten worden geïntegreerd in de bestaande netwerken voor de strijd tegen cybercriminaliteit op zowel Belgisch federaal als internationaal niveau. Er moeten contacten en samenwerkingen worden opgezet met:

- op Belgisch niveau: de Federal Computer Crime Unit en de Regional Computer Crime Unit
- op internationaal niveau: instanties zoals Interpol, de FBI, EC3 van Europol of de EUCTF (European Cybercrime Task Force)

2. IMPLEMENTATIE VAN HET CYBERVEILIGHEIDSPLAN

Omdat we meer dan een loutere analyse willen aanreiken, sommen we hieronder de stappen op die volgens ons noodzakelijk zijn voor een implementatie met de gewenste resultaten.

2.1. Oprichting van een gewestelijke studiegroep

Die studiegroep moet de belangrijkste actoren op het vlak van cyberveiligheid in het Brussels Hoofdstedelijk Gewest bij elkaar brengen om de acties in het kader van het in dit document beschreven cyberveiligheidsplan te onderzoeken en verder te ontwikkelen. De studiegroep zal vertrekken van de voor het GVPP door BPV opgerichte werkgroep en zal haar leden rekruteren in zowel de openbare als privésector (bedrijven, academische en onderzoekswereld).

De werkzaamheden van de studiegroep zullen erin bestaan:

- de voornaamste actoren te identificeren die een rol spelen in de cyberveiligheid in het Gewest, met inbegrip van het definiëren van hun rollen, verantwoordelijkheden en rechten;
- duidelijkheid te scheppen in de cyberveiligheidsbevoegdheden van het gewest en deze te onderscheiden van de bevoegdheden van het federaal niveau en de andere entiteiten van de federale staatsstructuur;
- een gewestelijk cyberveiligheidsprogramma samen te stellen met de beschrijving van concrete projecten voor elk van de krachtlijnen van het cyberveiligheidsplan;
- een cyberveiligheidsroadmap voor te stellen voor de periode tot 2020;
- de verwezenlijking van die roadmap op te volgen.

2.2. Een bestuursstructuur implementeren voor het gewestelijk cyberveiligheidsprogramma

Met het oog op de samenhang en de duurzaamheid van het cyberveiligheidsplan moet een bestuursstructuur met meerdere niveaus worden ingevoerd, met stevige ondersteuning van de Gewestregering, zowel op het vlak van visie als qua budget:

- de aansturing van het cyberveiligheidsplan door een comité van experts
- sectorcomités voor de implementatie en de opvolging van de roadmap

2.3. Publiek-privépartnerships opzetten

Bij de implementatie van de strategie moeten alle stakeholders op het vlak van cyberveiligheid in het Brussels Hoofdstedelijk Gewest worden betrokken. Er kunnen publiek-privépartnerships worden opgezet om de capaciteiten en expertise van de gewestinstanties te verbeteren wat de aanpak van kwetsbaarheden, incidenten en aanvallen in cyberspace betreft.

IN DE STRIJD TEGEN CYBERCRIMINALITEIT MOET MEN EEN BEROEP KUNNEN DOEN OP SPECIALISTEN

Het kan niet de bedoeling zijn dat de virtuele wereld minder bescherming biedt dan de werkelijke. Daarom moeten overheden de nodige kaders scheppen en stappen zetten om een vlot, veilig gebruik te garanderen van digitale tools en netwerken en de informatie die ze bevatten. De inzet is een vertrouwensklimaat waarin iedereen het meeste kan halen uit huidige technologieën, waarbij ieders persoonlijke levenssfeer en gegevens (in het bijzonder persoonsgegevens) doeltreffend worden beschermd tegen zowel onbedoelde inzage of verlies als tegen ultranationalistes.

Dit katern heeft tot doel de overheidsactoren en -besluitvormers van het Brussels Hoofdstedelijk Gewest en in bredere zin de Brusselse bedrijfs- en academische wereld bewust te maken van de uitdagingen op het vlak van cyberveiligheid in de huidige wereld die verregaand afhankelijk is van ICT. Op die manier wil het katern richting geven aan de acties van het Gewest, om de veerkracht van zijn informatiesystemen te waarborgen.

DE INZET IS EEN VERTROUWENSKLIMAAT WAARIN IEDEREEN HET MEESTE KAN HALEN UIT HUIDIGE TECHNOLOGIEËN

Naast het waarschuwingseffect van de herhaaldelijke cyberaanvallen hebben we getracht ook de verschillende dimensies van een toekomstig gewestelijk cyberveiligheidsplan in de kijker te zetten, met name preventie, reactie en herstel. Het plan is opgebouwd rond vier krachtlijnen:

- het organiseren van de cyberveerkracht van onze technische infrastructuren
- het ontwikkelen van de industriële, technologische en menselijke resources van het gewest
- het bevorderen van een cyberveiligheidscultuur, met name bij de Brusselse bevolking en bedrijven
- het voorkomen van cyberincidenten

Zoals de recente voorbeelden van cyberaanvallen in 2017 hebben aangetoond, is de onderlinge afhankelijkheid tussen informatiesystemen een verzwarende factor voor de risico's en dreigingen die voor de democratie op de loer liggen. Het gewest moet dus trachten overkoepelend te werk te gaan door actieve krachten te bundelen voor cyberveerkracht en de sterke punten van alle betrokken spelers inzetten. In het kader hiervan moeten de grenzen tussen de privé- en de openbare sector, de academische en de bedrijfswereld opgeheven worden zonder de individuele burgers te vergeten.

De eerste stenen van het gewestelijk cyberveiligheidsplan zijn al gelegd. Voor het CIBG vertaalt dat zich in beveiligde infrastructuren, informaticabeveiligingsdiensten en het in regel stellen van de Brusselse openbare besturen met de AVG. Voor het BPV staat het GVPP en aanverwante ontwikkelingen hier centraal. Al deze elementen garanderen een stevige basis voor een gewestelijk cyberveiligheidsplan in perfecte synergie met de taken van het CCB op federaal niveau.

De ambitieuze positionering van het gewest beantwoordt perfect aan de intelligente wisselwerking tussen de competenties voor zowel de ontwikkeling van informaticatools als de coördinatie van veiligheidsbeleidslijnen.

De tijd is rijp om de vruchten te plukken van deze eerste verwezenlijkingen. Het is nu aan de gewestregering om de passende besluiten te nemen en uit te voeren om het cyberveiligheidsplan waaraan het CIBG en BPV in dit katern gestalte geven tot leven te wekken. Onze beide organisaties staan klaar om het gewest te begeleiden bij deze opdracht en mee concreet vorm te geven aan het plan.

WOORDENLIJST

BBPV	Brussel Preventie & Veiligheid
CCB	Centrum voor Cyberveiligheid België
CERT	Computer Emergency Response Team
CIBG	Centrum voor Informatica voor het Brusselse Gewest
CSF	Cybersecurity Framework
IVA	Informatieveiligheidsadviseur
GDC	Gewestelijk Data Center
DNS	Domain Name System
DPO	Data Protection Officer
ENISA	European Network and Information Security Agency
FCCU	Federal Computer Crime Unit
GDPR	General Data Protection Regulation
ISaaS	Information Security as a Service
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IXP	Internet eXchange Point
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OIV	Opérateur d'Importance Vitale
AED	Aanbieder van Essentiële Diensten
GVPP	Globaal veiligheids- en preventieplan
Kmo	Kleine/Middelgrote Onderneming
RCCU	Regional Computer Crime Unit
ICT	Informatie- en communicatietechnologie
ZKO	Zeer kleine onderneming

DE KATERNEN VAN HET CIBG

Het Centrum voor Informatica voor het Brusselse Gewest heeft als taak het gebruik van informatie- en communicatietechnieken te organiseren, te promoten en te verspreiden zowel bij plaatselijke overheden als bij de verschillende besturen van het Brussels Hoofdstedelijk Gewest.

Het Centrum heeft binnen deze context als opdracht te informeren, met name door de publicatie van Katernen die een beeld vormen van zijn activiteiten, projecten of de evolutie van de technologieën.

RECENTE PUBLICATIES:

2017	
Praktische gids	AVG: praktische gids voor de gemeentelijke en gewestelijke instellingen van het Brussels Hoofdstedelijk Gewest
2015	
Katern 36	12 gouden regels inzake ICT-security
Katern 35	4 centrale projecten van smartcity.brussels
2014	
Witboek 2014-2019	Smart.brussels: een verbonden, duurzaam, open en veilig gewest
2013	
Katern 34	IRISnet, de ruggengraat van een Smart Region
2012	
Katern 33	Join the conversation: de overheid in het tijdperk van de sociale netwerken + Sociale Media praktische gids

De Katernen van het CIBG zijn beschikbaar in elektronisch formaat en te vinden op cibg.brussels.

Voor meer informatie stuurt u een mailtje naar communicatie@cibg.brussels

Redactie en coördinatie: Dienst Communicatie CIBG
Gedrukt met plantaardige inkt op papier afkomstig uit duurzaam beheerde bossen (FSC-label).

cibg.brussels
IT is for you

Verantwoordelijke uitgever : Hervé Feuillien
CIBG Kunstlaan 21 - 1000 Brussel
T 32 2 282 47 70 F 32 2 230 31 07
cibg.brussels - communicatie@cibg.brussels
@CIRB_CIBG