EVOLIRIS ZOOMT IN OP... #2

Schijnwerper op de Cyberveiligheid in Brussel;

DE SENSIBILISERING VOORBIJ

evoliris

"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."

John Chambers, Executive Chairman en CEO bij CISCO

Source : https://www.brainyquote.com/quotes/quotes/j/johntcham821369.html

Inhoudstafel

Voorwoord

De informatica is levendiger dan ooit. Evoliris tracht sinds zijn oprichting deze technologische evolutie op te volgen om de gevolgen en implicaties ervan op de arbeidsmarkt en in het onderwijs te begrijpen.

Elk jaar geeft de trendgrafiek van Gartner de evolutie weer van de technologische trends. In 2017* toonde deze analyse aan dat de Big Data, Artificial Intelligence, Internet of Things, de toegevoegde realiteit en cybersecuritytechnologieën volop in opmars zijn.

Wat de evolutie van de virtuele criminaliteit betreft, zien we dat Cybersecurity onrust creëert bij verantwoordelijken zowel in de IT als in de politiek en maatschappij. Talrijke Belgische, Europese en mondiale initiatieven tonen hoe belangrijk het is zich aan te passen aan, en de economische en sociale actoren bewust te maken van de bedreigingen op het internet.

En niet zonder reden: mei 2017 werd getekend door een aantal aanvallen van enorme omvang (onder andere Wannacry, NotPetya). Op zich niets nieuws ware het niet dat de media een grote rol is gaan spelen in het verspreiden van de informatie. Op slag werd de burger - u en ik - zich bewust van het feit dat onze virtuele wereld niet onfeilbaar is en dat de methodes waarmee men persoonlijke en gevoelige gegevens ontfutselt heel geavanceerd zijn.

Het is de opdracht van Evoliris, en binnenkort ook van de Opleidings- en Tewerkstellingspool voor ICT, om de sectorobservatie van o.a. Cybersecurity uit te werken, zodat de opleidingen die de pool voorstelt aangepast zijn aan de evolutie van de beroepen.

De bedoeling van dit document is om de impact en plaats van Cybersecurity in het Brussels Hoofdstedelijk Gewest te bestuderen in termen van economie, politiek, tewerkstelling of onderwijs. De (Europese, federale of regionale) politieke acties, het informatiebeveiligingsbeheer binnen bedrijven, de academische sector en de analyse van de aanwervingen zijn belangrijke factoren in de evolutie van de Cybersecurity in Brussel. Met de hulp van Belgische experten konden we dit document opstellen met voeling voor de realiteit van het terrein.

De sensibilisering, het gemengd karakter, de federale of Europese voorschriften, de beroepsprofielen en het opleidingslandschap in Brussel zijn allemaal onderwerpen die we in dit tweede rapport "**Evoliris zoomt in op**" hebben uitgewerkt. Veel leesplezier!

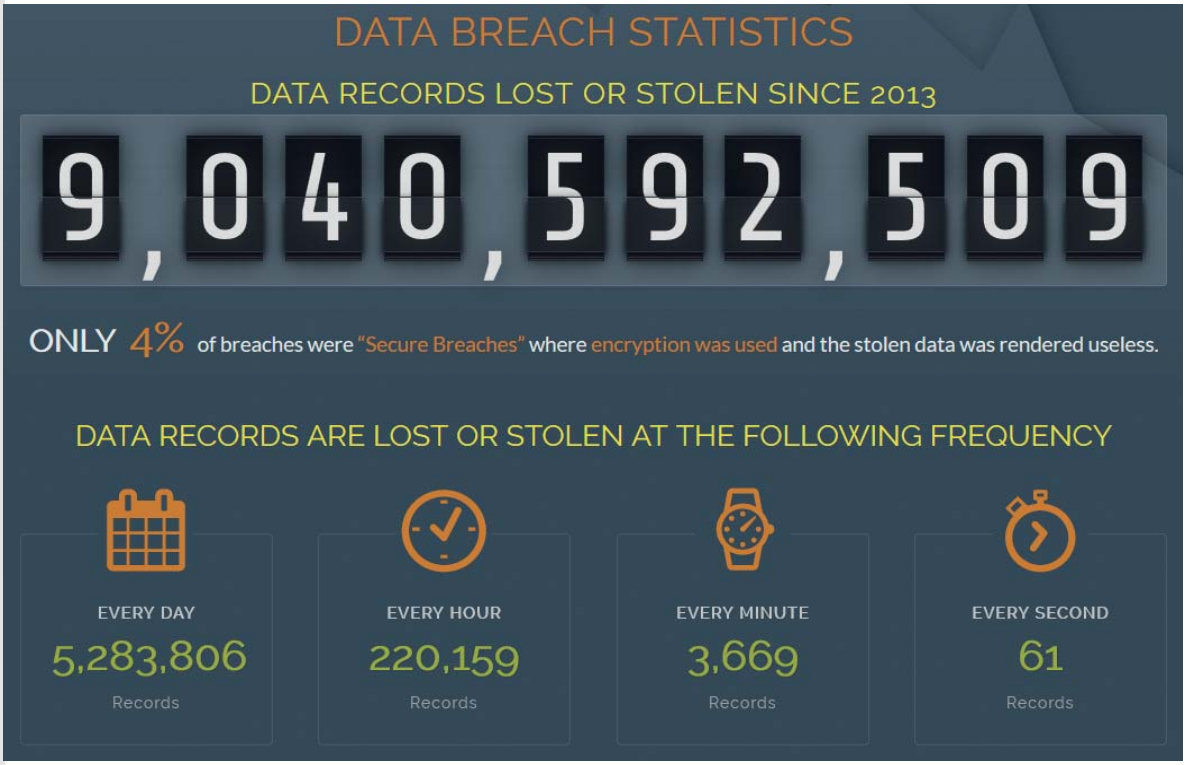
Jean-Pierre Rucci
Directeur van Evoliris

Pierre Merveille
Voorzitter van Evoliris & verantwoordelijke secretaris aan de BBTK voor de sectoren Financiën - Diensten - Industrie

* https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

1 Inleiding

Wereldwijd worden dagelijks meer dan 5 miljoen gegevens gestolen of verloren, dat zijn meer dan 200 000 gegevens per uur[1].
In België werd in 2009 reeds voor 68 miljoen euro schade wegens fraude veroorzaakt, volgens de Federal Computer Crime Unit (FCCU) [2].



Figuur 1 - Breach Level Index. Bron: http://breachlevelindex.com

Deze cijfers tonen duidelijk aan dat Cyberbeveiliging, de beveiliging van gegevens, een echte uitdaging is. Het is niet alleen een uitdaging op **technologisch** gebied met de ontwikkeling van krachtige tools om aanvallen te detecteren, het is ook een **politieke** uitdaging. Het almaar stijgend aantal aanvallen dwingt alle landen over de hele wereld om strategieën voor Cyberbeveiliging op nationaal niveau in te voeren. Ten slotte is het ook een **economische** en **maatschappelijke** uitdaging want de beroepen die al dan niet in nauw verband staan met de beveiliging zijn in volle opmars. Vandaag is alles digitaal. En dat hebben de hackers maar al te goed begrepen.

We lezen bijna dagelijks in de krant over een ernstige veiligheidsinbreuk of gegevensdiefstal. De namen *WannaCry*[3] *en NotPetya*[4], klinken u vast niet onbekend in de oren.

Meer lokaal treft de Cyberveiligheid de Brusselse bedrijfseconomie, de beroepen en het onderwijs. Het is een thema dat onrust wekt vooral op federaal niveau maar ook in de overheidssector, in bedrijven en bij de burgers.

1. http://breachlevelindex.com
2. « La Cybersécurité est un enjeu pour tous » door Gaëtan in LaLibre.be [online] http://www.lalibre.be/economie/digital/la-cybersecurite-est-un-enjeu-pour-tous-51b732d1e4b0de6db9756ab2
3. Wannacry : zie woordenlijst.
4. NotPetya : zie woordenlijst.

1.1 Waarom de Cyberbeveiliging in Brussel bestuderen ?

Sectorobservatie is een van de opdrachten van Evoliris. De beweegreden achter deze opdracht is om opleidingen aan te bevelen, aanbevelingen te formuleren of advies te verstrekken die aangepast zijn aan de huidige vereisten van de sector.

Het uiteindelijke doel van deze "Evoliris zoomt in op…" is om de situatie van de Cyberbeveiliging in het Brusselse Gewest te schetsen. Het is immers interessant om de impact van cyberdreigingen in Brussel te analyseren in termen van opleidingen, beroepen en veiligheidsbeheer binnen bedrijven. Bijgevolg kunnen we zien hoe Brussel aan de hand van haar beleid, maatregelen in de ICT-sector en opleidingen, reageert om het hoofd te bieden aan deze nieuwe vorm van bedreiging en hoe het Brussels Hoofdstedelijk Gewest zal moeten evolueren in de komende jaren. In 2013 verklaarde eerste minister Elio Di Rupo nog over de oprichting van het Centrum voor Cyberveiligheid België[5]: *"Veiligheid betekent ook de bescherming van het privéleven, van onze economische belangen en van het Staatsapparaat*[6]". Aan de hand van de conclusies van dit verslag kunnen we de situatie van Brussel tegenover dit probleem begrijpen en kunnen we toekomstgerichte acties voorstellen.

1.2 De aanpak

Om de hoofdlijnen uit te tekenen organiseerde Evoliris een ronde tafel met Cybersecurityexperten. Deze ronde tafel werd georganiseerd op 31 mei 2017. Ze bestond uit twee leden van Evoliris en 5 experten:

- Bruno Schröder Microsoft
- Amira Zoukani CEFORA
- Jean-Marc André UNIWAN
- Philip Richardson Bruxelles formation
- Thierry Cools Bruxelles formation

Tijdens deze ronde tafel hebben we tal van vragen kunnen stellen en zijn we tot heel wat vaststellingen gekomen waar we in dit verslag verder op ingaan. Om deze vragen verder uit te diepen hebben we daarna nog aparte gesprekken gevoerd met andere experten (de lijst van geraadpleegde experten is beschikbaar aan het einde van dit verslag in het hoofdstuk "Dankbetuigingen"). Op basis van deze gesprekken hebben we dit samenvattend verslag opgesteld. Bovendien worden op het einde van dit verslag conclusies en aanbevelingen voorgesteld.

In dit document stellen wij aan de hand van verschillende denkpistes uit de realiteit op het terrein, een inventaris op die vertrekt van een aantal vragen:

- Hoe belangrijk is de problematiek van de Cyberveiligheid in het Brussels Hoofdstedelijk Gewest?
- Welk maturiteitsniveau heeft Brussel?
- Hoe beïnvloedt de Cyberveiligheid het Brusselse beroepenlandschap?
- Welke competenties zoekt men in de profielen van Cybersecurity?
- Welke maatregelen worden genomen door en voor de ondernemingen?
- Welke middelen gebruikt men om ondernemingen en burgers te sensibiliseren?
- Hoe beantwoordt de opleidingssector de nood aan aanwervingen in informatiebeveiliging?

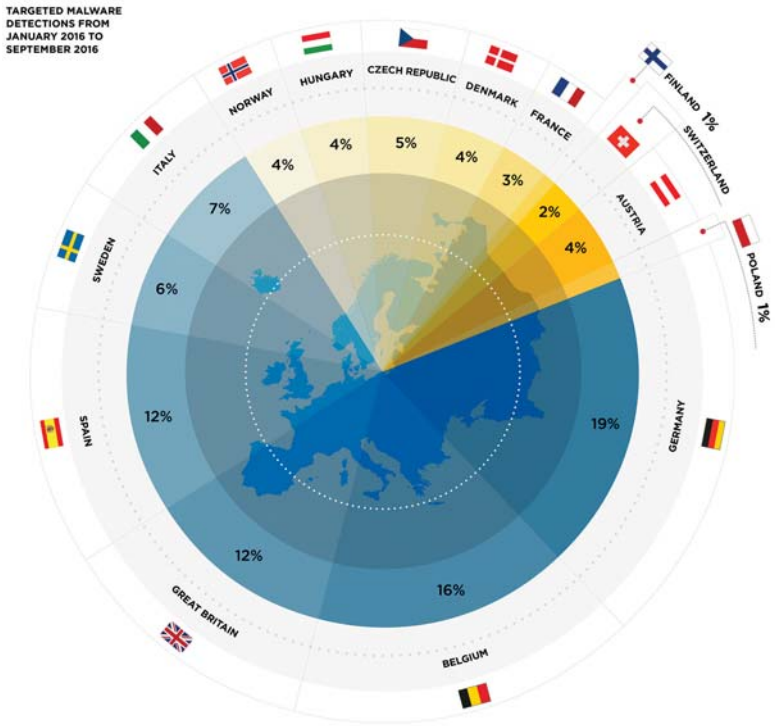
5. http://www.ccb.belgium.be/nl
6. http://home.scarlet.be/~pp155058/Cybersecurite.pdf

1.3 De Cyberveiligheid: afbakening van het onderwerp

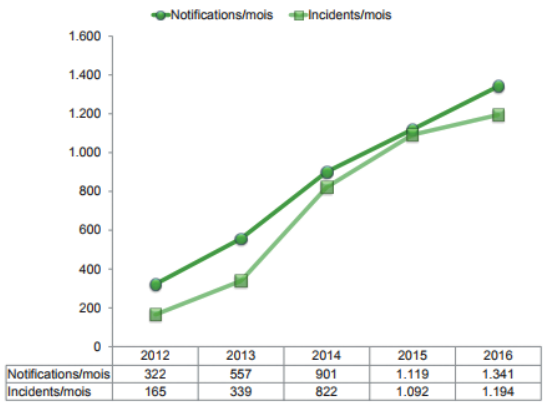
Cybersecurity is een generieke term die de problematiek omvat van verschillende soorten computeraanvallen, waarbij rekening gehouden wordt met de steeds meer aanwezige digitalisering en het almaar stijgend aantal bedreigingen.

Men schat dat België momenteel 16% vertegenwoordigt van de malware[7] aanvallen in Europa. Dat betekent dat België het tweede meest aangevallen land is na Duitsland volgens de grafiek op figuur 2. De sectoren die het meest door deze aanvallen worden getroffen zijn:

- De financiële sector,
- De profit sector,
- De overheid[8].



Figuur 2 - Bedreiging Malware detecties van januari 2016 tot september 2016. Bron : https://www2.fireeye.com/rs/848-DID-242/images/Infographic_GDPR.pdf



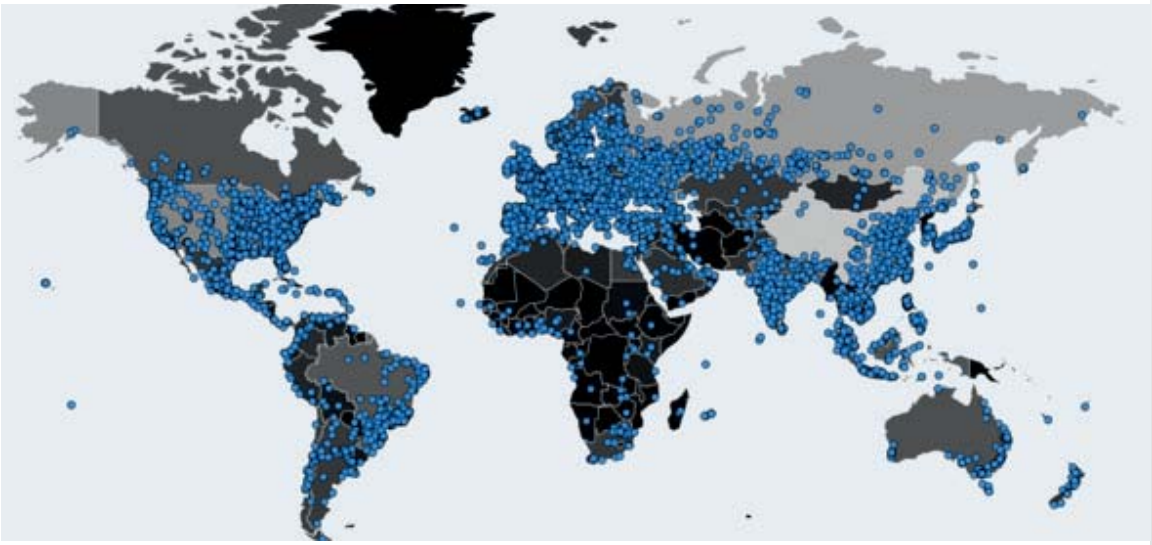
	2012	2013	2014	2015	2016
Notifications/mois	322	557	901	1.119	1.341
Incidents/mois	165	339	822	1.092	1.194

We merken ook op dat het aantal incidenten dat gerapporteerd wordt door BELNET sinds 2012 constant blijft stijgen[9].

Figuur 3 - aantal meldingen en reële incidenten (per maand). Bron BELNET

Het is nochtans dankzij aanvallen met een omvang zoals (onder andere) WannaCry of NotPetya dat we het probleem via de pers hebben leren kennen. Sensibiliseringsacties worden op poten gezet om de impact van deze bedreigingen te reduceren. Maar is dat voldoende?

7. Malware : zie woordenlijst
8. https://www2.fireeye.com/rs/848-DID-242/images/Infographic_GDPR.pdf
9. http://economie.fgov.be/nl/binaries/Barometer_van_de_informatiemaatschappij_2017_tcm325-284038.pdf



Figuur 4 - Bron afbeelding: MalwareTech.com

In mei 2017 maakte de aanval van de WannaCryWannaCry-ransomware wereldwijd meer dan 300.000 slachtoffers[10].

WannaCry is een ransomware[11] die een softwarefout van Microsoft Windows gebruikt. Deze ransomware heeft zich waarschijnlijk verspreid via een massale mailingcampagne. Eens het virus is geïnstalleerd en de bestanden versleuteld, vraagt het virus losgeld in bitcoins.

WannaCry heeft heel wat grote kritieke of belangrijke instellingen getroffen zoals Britse ziekenhuizen of het Russische Ministerie van Binnenlandse Zaken. Men schat dat 150 landen door deze malware werden getroffen. Volgens Europol werden 200 000 computers getroffen door het virus[12].

In België bleef de impact beperkt. Enkele kmo's hebben het CCB (Centrum voor Cyberveiligheid België) gecontacteerd. De onderneming Q-Park werd getroffen[13].

1.4 De Cybercriminaliteit, een verhaal dat reeds in de jaren '80 begon

Bij deze krijgt u dus een volledig verslag over Cybercriminaliteit of Cybercrime. Maar wat is dat nu precies? Als we Wikipedia mogen geloven is Cybercrime *een nieuwe vorm van criminaliteit en delinquentie die zich van de klassieke criminaliteit onderscheidt omdat het zich afspeelt in een virtuele wereld, de "cyberspace". Sinds enkele jaren zijn de gemakkelijke toegang tot informatie en de globalisering van de netwerken factoren die de ontwikkeling van Cybercriminaliteit hebben gestuwd*[14]. De realiteit is toch heel wat complexer.

Oorspronkelijk werden computers, netwerken en internet gecreëerd om informatie uit te wisselen in een virtuele ruimte die de fysieke grenzen overschrijdt. De (persoonlijke, bank-, beroeps-) gegevens worden een commerciële inzet voor heel wat oneerlijke individuen.

10 « Ransomware: le nettoyage se poursuit après le chaos WannaCry », ZDNet France, 2017 [online] http://www.zdnet.fr/actualites/ransomware-le-nettoyage-se-poursuit-apres-le-chaos-WannaCry-39852650.htm
11. Ransomware : zie woordenlijst.
12. https://www.rtbf.be/info/medias/detail_la-cyber-attaque-mondiale-pourrait-faire-de-nouvelles-victimes-ce-lundi?id=9606062
13. http://www.sudinfo.be/1844305/article/2017-05-15/les-parkings-q-park-touches-par-la-cyberattaque-les-conducteurs-peuvent-sortir-s
14. https://nl.wikipedia.org/wiki/Computercriminaliteit

De winsten die gehaald worden uit identiteitsdiefstal, diefstal van bankgegevens en andere beroepsgeheimen, hebben een meer dan winstgevende industrie gecreëerd.

De cybercriminaliteit stak de kop op in de jaren '80 maar toen werd u nog niet online bestolen. U herinnert zich ongetwijfeld de Nigeriaanse prins die uw hulp en geld vraagt om een gigantische geldsom vrij te krijgen die in Engeland wordt geblokkeerd. Om u voor uw inspanning te bedanken belooft de weldoener u 10% van deze mooie som.

Vervolgens kwam de scam via browsers die veiligheidsgebreken vertoonden. U bezocht een site (vaak een niet aanbevolen site, moeten we toegeven) die iets in uw browser installeert waardoor u plots tal van "pop-ups[15]" zag verschijnen.

Maar in de jaren '90 werd het pas menens met de komst van het World Wide Web in 1994. Op dat ogenblik hebben de internetcriminelen ontdekt dat websites (beheerders van inhoud) databanken van persoonlijke gegevens (van bijvoorbeeld klanten, leden of bezoekers) bevatten. Het was heel gemakkelijk om vanuit de webinterface van de organisatie toegang te krijgen tot deze databanken. Voor de cybercriminelen was dit een echte grot van Ali Baba.

In dit hoofdstuk hebben we het nog niet over virussen gehad. Het is nochtans het eerste woord dat ons te binnen schiet als we over Cybercriminaliteit praten. Er was een tijd dat men zich amuseerde met het verspreiden van virussen om mensen te plagen. Het virus "Elk Cloner[16]" is een van de eerste virussen die voor de Apple II (1982) werd ontwikkeld. Daarna volgen tal van virussen elkaar op, en ze worden steeds kwaadaardiger.

In de loop der jaren volgen meerdere grapjassen elkaar op om de Koreaanse nucleaire programma's te kraken, de NASA en andere internationale organisaties zoals de CIA. Daarna volgen de macrovirussen die de macro-talen van applicaties gebruiken en zichzelf dus opstarten zodra u uw applicaties opent. En dat is nieuw, want voordien waren virussen nog aparte programma's.

De geschiedenis van de cybercriminaliteit staat rechtstreeks in verband met de evolutie van de informatietechnologieën. Deze evolutie blijft maar voortduren en wordt steeds complexer. Dit kort hoofdstuk is slechts een voorsmaakje. Wilt u hier meer over weten? Lees dit artikel[17] waarin de voordelen van de VPN verbinding worden besproken, en dit artikel[18], waarin Symantec, een van de grootste spelers in beveiliging, de geschiedenis van de cybercriminaliteit uit de doeken doet.

De cybercriminaliteit heeft een rijk verleden, en een mooie toekomst voor zich. Nu zullen we de impact bekijken van de cybercriminaliteit en de Cyberveiligheid in Brussel.

15. Pop-Up : zie woordenlijst.
16. https://en.wikipedia.org/wiki/Elk_Cloner ==> https://nl.wikipedia.org/wiki/Elk_Cloner
17. https://www.le-vpn.com/fr/cybercriminalite-origines-evolution/
18. http://www.symantec.com/region/fr/resources/cybercrime.html

Een Brusselse economie van Cybersecurity

2

- 5 punten om de maturiteit van het Gewest te evalueren -

Tijdens de gesprekken met de experten werd de mogelijkheid aangekaart dat het Brussels Hoofdstedelijk Gewest een Europese stad van Cybersecurity kan zijn. In dit rapport zullen we deze problematiek inschatten aan de hand van 5 belangrijke punten uit de Brusselse politiek en economie.

2.1 Wat politici willen

We vroegen ons af welke acties het Brussels parlement onderneemt op het niveau van informatiebeveiliging.

Volgens de heer Nicolas Harmel, attaché bij het kabinet van de heer Didier Gosuin, minister van Economie, Tewerkstelling, Opleiding, Gezondheid, Budget en Openbaar ambt "*is, in de context van de regionalisering, de kwestie rond Cyberveiligheid nog steeds sterk versnipperd. De meeste acties worden doorgevoerd via het CIBG (Centrum voor Informatica voor het Brusselse Gewest)*".

Maar "*aangezien overheidsinstellingen steeds vaker het doelwit worden van georganiseerde aanvallen, komt het onderwerp toch steeds meer aan bod in het parlement*" vertelt de heer De Lestré, adviseur Informatica en Digitalisering aan het kabinet van staatssecretaris Bianca Debaets die verantwoordelijk is voor Informatica en Digitalisering.

De Brusselse parlementsleden zijn voornamelijk bezorgd om de veiligheid van de infrastructuur die de systemen en openbare databanken host. Ondanks initiatieven zoals het NextTech[19] plan vinden ze dat sensibiliseringscampagnes niet hun taak zijn. Met het NextTech plan wil men de problematiek rond Cybersecurity aankaarten en de mensen sensibiliseren. Maatregel 16, over de oprichting van de Opleidings- en tewerkstellingspool voor ICT, wil opleidingen en werkgelegenheid in de Brusselse IT-sector creëren en toegankelijk maken. De pool bestudeert de sector zodat de voorgestelde opleidingen worden aangepast aan de evolutie van de beroepen. De beroepen in Cyberveiligheid evolueren echter constant en dit zal de komende jaren niet veranderen. Als we de rekruteringsgegevens bekijken zien we dat er een groeiend tekort is aan gekwalificeerde profielen. Tegen 2020 zal België met een tekort kampen van 2000 Cybersecurityexperten[20]. Met opleidingen en promotie van de sector zou de pool een antwoord kunnen bieden aan de behoeften van Brussel inzake maturiteit.

Wat het institutionele landschap betreft, moeten we een onderscheid maken tussen de regionale en federale bevoegdheden. Traditioneel valt het beheer van Cyberveiligheid en Cybercriminaliteit onder de federale bevoegdheden die maatregelen invoeren om de veiligheid te verhogen. "*Het is ondertussen duidelijk dat de Cyberveiligheid meer een federale dan regionale aangelegenheid is." Toch moet het Gewest meewerken aan deze opdracht"* verklaart de heer Ferdinand Casier, Business Group Leader Digital Industries bij Agoria.

19. https://nexttech.brussels/?lang=nl
20. https://www.digitalwallonia.be/centre-cybersecurite-thales/ /

2.2 Oprichting van het CCB en centralisatie van de federale instanties

Op federaal niveau werd actie ondernomen door het CCB (Centrum voor Cybersecurity België [21]) op te richten, waar de acties rond Cybersecurity gecentraliseerd worden. Met ondersteuning van de dienst CERT.be beheert het CCB crisissituaties die verband houden met cyberaanvallen en geeft het aanbevelingen inzake beveiliging van informatiesystemen en -netwerken in de overheidssector en aan openbare nutsbedrijven. Deze aanbevelingen dienen om het voorbereidend werk te faciliteren en om zowel publieke als privéinstellingen zich te helpen wapenen tegen cyberaanvallen en te laten weten wie ze moeten contacteren in geval van nood. Het CCB moet de instellingen ook bewust maken van de beveiligingspraktijken en van de beschikbare Belgische bijstand en hulpmiddelen.

"*We moeten de informatie centraliseren! Doel is om een referentieplatform voor ondernemingen en een referentieplatform voor het grote publiek te creëren*" zegt de heer Olivier Bogaert van de FCUU (Federal Computer Crime Unit). Deze verklaring van de heer Bogaert benadrukt de voornaamste doelstelling van het CCB: de federale actoren van Cyberveiligheid samenbrengen om een uniek informatieplatform voor te stellen dat zal dienst doen als referentie.

Focus op het CCB

CENTRE FOR CYBER SECURITY BELGIUM

Het Centrum voor Cyberveiligheid België (CCB) is opgericht bij Koninklijk Besluit van 10 oktober 2014 en is de bevoegde nationale autoriteit inzake beveiliging van informatiesystemen en -netwerken in België. Zijn opdracht bestaat uit het coördineren en centraliseren van projecten en beleidslijnen inzake Cyberveiligheid. Sinds 2017 wordt de dienst CERT.be ("Computer Emergency Response Team", het federale cyber urgentieteam), vroeger in handen van BELNET, beheerd door het CCB. Het CCB hecht veel belang aan de sensibilisering van het publiek. Daarom organiseert het elk jaar een nationale sensibiliseringscampagne. In 2017 was het thema van de campagne de bestrijding van "Phishing".

Op de website van het CCB en CERT.be vindt men brochures en nuttige tips. Deze zijn bedoeld voor alle soorten publiek: burgers, ondernemingen, scholen, publieke instellingen en vitale sectoren (energie, mobiliteit, gezondheidszorg, financiën, etc.).

www.ccb.belgium.be I www.cert.be I www.safeonweb.be

2.3 Europa inspireert

Ook op Europees niveau is Cybersecurity een hot topic geworden. In 2016 lanceerde de Europese Commissie een project van publiek-private samenwerking waarbij ze 450 miljoen euro heeft geïnvesteerd voor onderzoek en verdere ontwikkeling van Cybersecurity[22]. De privésector moet tot 2020 1,35 miljard investeren in de projecten. De financiering werd in 2013 aangevat met een nota over de "Strategie van Cyberveiligheid van de Europese Unie[23]".

Deze nota omvat vijf belangrijke doelstellingen:

- *"cyberveerkracht vinden;*
- *cybercriminaliteit aanzienlijk reduceren;*

21. http://www.ccb.belgium.be/fr
22. Cybersécurité : Bruxelles investit 450 millions d'euros, dans Les numériques [en ligne] consulté le 28 août 2017 http://www.lesnumeriques.com/vie-du-net/cybersecurite-bruxelles-investit-450-millions-euros-n53807.html
23. http://www.consilium.europa.eu/fr/policies/cyber-security/
24. Cyber-résilience : zie woordenlijst

- *een beleid rond cyberdefensie en capaciteiten uitwerken die vallen onder het gemeenschappelijk veiligheids- en defensiebeleid van de EU (GVDB);*
- *industriële en technologische ressources ontwikkelen die vereist zijn voor Cybersecurity;*
- *een coherent internationaal beleid inzake cyberspace invoeren voor de EU[25]".*

Kortom, de Europese acties zijn opgebouwd rond meerdere assen:

- **Advies en sensibilisering :** met acties zoals de *European Cyber Security Month[26] (of CyberSecMonth)*. Elk jaar in oktober (sinds 2012) organiseert de Europese Commissie sensibiliseringsprojecten voor Cyberveiligheid. Over heel Europa worden sensibiliserings-activiteiten en –evenementen georganiseerd,
- **Invoering van maatregelen en voorschriften om de Cyberbeveiliging te structureren:** de Europese Commissie heeft structurerende maatregelen voor bedrijven ingevoerd zoals de GDPR-wetgeving (General Data Protection Regulation, ofte AVG, *Algemene Verordening Gegevensbescherming* in het Nederlands) en de NIS-richtlijn (Network and Information Security) die we in een later hoofdstuk gedetailleerder zullen bespreken (zie 4.4.1 Network and Information Security - NIS op pagina 24),
- **Centralisatie van Europese hulpmiddelen en acties:** In september 2017 heeft de Europese Commissie een nieuw agentschap voor Cyberbeveiliging[27] voorgesteld. Dit agentschap, gebaseerd op het Europees Agentschap voor Netwerk- en Informatiebeveiliging (Enisa), kan certificaten uitreiken die de betrouwbaarheid van de betreffende digitale diensten en producten garanderen.

Uiteindelijk blijkt uit deze acties dat de Europese Commissie een strategisch plan op Europees niveau wil invoeren om een Europees referentiepunt voor de lidstaten te creëren.

2.4 De opleidings- en tewerkstellingspool voor ICT : de economische rol van opleidingen

Er is momenteel een grote kloof tussen de beschikbare gekwalificeerde profielen op de Belgische arbeidsmarkt en het stijgend aantal vacatures. Dit probleem wordt beïnvloed door het gebrek aan opleidingen in Cyberveiligheid in België. De huidige opleidingen leveren niet voldoende experten in Cyberveiligheid af om te kunnen voldoen aan de vraag van de sector. Dit is geen ongekend probleem, en daarom worden sinds enkele maanden verschillende nieuwe opleidingen in het leven geroepen. Universitaire opleidingen, bachelors, geïntegreerde lessen in vernieuwde programma's of kwalificerende opleidingen, er zijn tal van nieuwe mogelijkheden om toegang te krijgen tot een beroep in volle opmars. Deze opleidingen moeten wel de competenties kunnen bieden die overeenstemmen met de behoeften van de ondernemingen. 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.

De opleidings- en tewerkstellingspool is voorzien tegen eind 2018 en wordt financieel ondersteund door zowel de publieke als de private sector. De opleidings- en tewerkstellingspool komt er omdat de regionale politiek een instelling wilt oprichten die de actoren van opleiding en tewerkstelling in de IT-sector centraliseert. De pool zal dus moeten *"de organisatie versterken, opleidingen en tewerkstelling in de beoogde sector ontwikkelen*

25. http://www.consilium.europa.eu/nl/policies/cyber-security/
26. https://cybersecuritymonth.eu/
27. http://datanews.levif.be/ict/actualite/une-nouvelle-agence-europeenne-de-cyber-securite-en-chantier/article-normal-725497.html

en promoten, en het publiek sensibiliseren voor ICT beroepen, ter ondersteuning van de economische en sociale ontwikkeling van het Brusselse grondgebied[28]".

2.5 Brussel is nog niet klaar om de hoofdstad van Cybersecurity te worden

Om dit verslag voor te bereiden hebben we heel wat gesprekken gevoerd. Daaruit is een merkwaardig beeld van Brussel gekomen. Tal van onze gesprekspartners wezen ons, bijvoorbeeld, op de symbolische waarde die Brussel heeft als Europese hoofdstad.

De Belgische hoofdstad mag dan wel klein zijn in omvang maar toch hebben zich hier tal van belangrijke Europese instellingen gevestigd; de Europese Commissie en Parlement, de NAVO, Eurocontrol. Op hun beurt hebben deze ervoor gezorgd dat verschillende wereldorganisaties zich zijn komen vestigen; de Raad van Europa, de VN, UNESCO, de Wereldbank, enzovoort. Deze beau monde trekt dan weer heel wat bedrijven aan die op de een of andere manier afhankelijk zijn van deze internationale organisaties. Natuurlijk heeft dit verhaal ook een donker kantje want op die manier gaan cybercriminelen ook belangstelling krijgen voor onze hoofdstad.

En net daar wringt het schoentje: momenteel voldoet Brussel niet aan de vereiste voorwaarden om een Cybersecurity hoofdstad te worden. De stad is hier nog niet rijp voor. We tonen dit aan en verklaren aan de hand van deze vijf punten (waarover later meer):

- Interessante Europese acties, maar vaag,
- Gecentraliseerde federale actie maar weinig zichtbaarheid,
- Regionale bezorgdheden beperkt tot overheidsinstellingen,
- Grote kloof tussen aanbod van Belgische beroepsprofielen en aantal vacatures, gedeeltelijk te wijten aan tekort aan opleidingen in Cyberveiligheid,
- Opleidingen in Cyberveiligheid te weinig gekend op academisch niveau.

Dit zal in de toekomst snel moeten evolueren en gelijklopen met de behoeften van de sector. Het wordt vast interessant om over enkele jaren opnieuw te polsen naar de maturiteit van Brussel op dit gebied.

28. https://nexttech.brussels/globaal-overzicht-van-ict-opleidingen/?lang=nl

Sensibiliseren, opleiden, reageren op bedreigingen

- op weg naar een veilige maatschappij -

3

3.1 Sensibilisering: geen gemakkelijke taak

In 2010 werden 62,7% van de Belgen het slachtoffer van cybercriminaliteit[29]. De aanvallen zijn steeds beter georganiseerd en heel wat burgers laten zich vangen. Daarom is sensibilisering een maatschappelijke uitdaging.

Er bestaan in België verschillende initiatieven en voorlichtingscampagnes. We denken hierbij in de eerste plaats aan de talrijke conferenties en *white papers*[30] die we overal op het internet en in het land zien opduiken. Deze initiatieven draaien rond het gebruikersvriendelijk communiceren van gouden raad, goede praktijken en richtlijnen. Ze is vooral gericht op een publiek dat zelf informatie opzoekt over het onderwerp en zelf op de site of pagina van een evenement is beland. Maar wat doen we met diegenen die menen dat beveiliging niet aan hen besteed is? Met welke middelen kunnen we hen sensibiliseren? Ondanks diverse voorlichtingscampagnes blijft de burger moeilijk te overtuigen. Volgens de heer Olivier Bogaert van de FCCU "*bevinden we ons in een kantelperiode. De gewoonten zullen veranderen. We moeten de leerkrachten en ouders sensibiliseren zodat ze hun kinderen de basisveiligheidsmaatregelen op internet bijbrengen*".

Bovendien moeten we ons ook afvragen hoe doeltreffend de bewustwordingscampagnes zijn die op het internet, in de pers en op reclameschermen te zien zijn. Laten we even de campagne "Take back the internet[31]" als voorbeeld nemen, die het CCB in oktober 2016 heeft gevoerd om het platform **Safe**on**web**[32] te promoten. Volgens het CCB werd tijdens de periode van deze campagne de website door anderhalf miljoen internetgebruikers bezocht, waarvan 88% voor de eerste keer. 200 000 bezoekers deden de veiligheidstest. In navolging van deze campagne steeg het aantal automatische virusscans vooral op professionele laptops en computers met 14%. Deze campagnes hebben dus wel degelijk een positieve impact maar de beveiligingsincidenten worden steeds frequenter en dat creëert een andere vraag: Hoe kunnen we ervoor zorgen dat de bezoekers dagelijks veilig internetten in plaats van af en toe? Eigenlijk is het niet moeilijk: we moeten de veiligheidsregels constant herhalen zodat ze een gewoonte worden. "*Denk maar aan het gebruik van de veiligheidsgordel in de wagen. Hoe vaak hebben onze ouders niet herhaald dat we onze gordel moeten omdoen zodra we in de wagen stappen? Nu, als volwassene, is deze handeling na al die jaren een normale handeling geworden, een gewoonte*", verklaart de heer Bogaert van de FCCU.

De overheid heeft binnen dit kader een adviserende en begeleidende rol te vervullen. "*De overheid moet het voorbeeld geven*" verklaart de heer Vautrin van Innoviris. Er bestaan namelijk incubatoren, projecten zoals Impulse.Brussels[33] of het informatieplatform 1819[34] waar startups of kleine ondernemingen terechtkunnen voor begeleiding en advies.

Bovendien benadrukt de heer Grégorio Matias van MCG *"dat we de manier van communiceren moeten personaliseren en variëren in functie van de verschillende doelgroepen".*

29. http://www.lalibre.be/economie/digital/la-cybersecurite-est-un-enjeu-pour-tous-51b732d1e4b0de6db9756ab2
30. White paper : zie woordenlijst.
31. http://www.ccb.belgium.be/nl/news/resultaten-bewustwordingscampagne-2016
32. https://www.safeonweb.be/nl
33. http://www.abe-bao.be/nl
34. http://www.1819.be/nl/page/over-1819

Wat zijn de oplossingen om de verschillende soorten publiek te bereiken en te sensibiliseren? Hoe kunnen we de verschillende soorten publiek apart bereiken: kinderen, bedrijfsleiders, werknemers, burgers? Het werkterrein is behoorlijk breed …

3.2 De ondernemingen sensibiliseren

Zoals de statistieken hieronder aantonen gaat het goed met de omzet van de economische activiteiten in de Belgische IT-sector en de omzet blijft stijgen sinds 2013.

Indexcijfer van de omzet per jaar, trimester, en economische activiteit (NACE 2008) volgens de btw-aangiftes

Jaar	2013	2014	2015	2016				2017
Trimester				1er trim.	2eme trim.	3eme trim.	4eme trim.	1er trim.
	bruto index	bruto index	bruto index	bruto index	bruto index	bruto index	bruto index	bruto index
Niveau 1 - NACE 2008								
J62 Programmeren, computerconsultancy en aanverwante activiteiten	115,64	125,75	137,15	142,45	142,8	132,46	168,59	150,02

Bron: omzet in de dienstensector (volgens btw). Algemene Directie Statistiek - Statistics Belgium[35].

Wat de veiligheid binnen bedrijven betreft, moeten we twee zaken apart bekijken.

1. Er zijn twee soorten ondernemingen: IT-ondernemingen en andere. Net als de bedrijven met IT als core business, werven de niet-IT-bedrijven heel wat IT-profielen aan (bijvoorbeeld banken, verzekeringen, etc.) en zijn ze dus belangrijke aanbieders van IT-jobs,
2. De veiligheid heeft niet dezelfde impact in een grote onderneming als in veel kleinere ondernemingen zoals kmo's, microbedrijven of startups. Niet alleen de financiële middelen zijn er anders, maar ook de materiële en menselijke middelen verschillen. De communicatie naar deze twee categorieën moet apart gebeuren en onderverdeeld worden in twee assen: de grote ondernemingen en de kmo's.

3.2.1 Grote ondernemingen

Over het algemeen zijn de grote ondernemingen zich reeds bewust van de problematiek rond Cyberveiligheid. De gegevens die ze verwerken hebben vaak een aanzienlijke economische waarde. In de gevallen waar het management de problematiek erkent, komt het gevaar vaak en ook ongewild van een slordige werknemer. De menselijke factor blijkt één van de hoofdoorzaken te zijn van veiligheidsinbreuken binnen bedrijven. Er is dus ook nog heel wat werk voor de boeg wat sensibilisering en communicatie voor de grote ondernemingen betreft. De onderneming moet zelf een veiligheidscultuur bewerkstelligen bij haar werknemers (*Cyber Security Policy*). Vaak zijn eenvoudige tips voor goede praktijken en preventie voldoende om een onderneming goed te laten functioneren. Sommige ondernemingen testen hun werknemers soms door ze "in de val te lokken". De werknemers die zich lieten vangen worden nadien begeleid om hun fouten te analyseren en ze worden verzocht deze fouten niet meer te maken. Maar "*Deze praktijk veroorzaakt een ethische kwestie. In dit geval wordt de werknemer die een fout beging in het bijzijn van zijn collega's op de vingers getikt*" vertelt de heer Rousseaux van Digital Security. We moeten de resultaten anoniem maken. De heer Pascal Van de Walle, CISO bij het CIBG, bevestigt dat testen binnen een bedrijf een troef zijn maar hij dringt er ook op aan dat de ondervraagden anoniem moeten blijven. Hij verduidelijkt: "*Het heeft geen enkele zin om de werknemers en hun fouten in de kijker te zetten, men moet de oorzaken van het probleem uitleggen en*

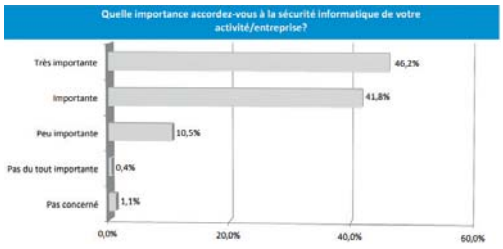
35. http://statbel.fgov.be/fr/statistiques/chiffres/economie/indices/chiffreaffair/

oplossingen voorstellen". Vaak zijn regelmatige opleidingen nodig die de regels van correct gebruik van gegevens herhalen. Tijdens ons gesprek benadrukt de heer Rousseaux dat sensibilisering op een speelse manier moet gebeuren. In zijn onderneming, Digital Security, werd een interessante formule bedacht om de beveiliging van zijn bedrijf te testen: de Red Team Attack[36]! De bedoeling is om de beveiliging van de onderneming te omzeilen en daarvoor mogen alle mogelijke middelen gebruikt worden (valse e-mails, fysiek binnendringen in het gebouw, etc.). Dit eindigt meestal heel grappig met de expert van Digital Security die een selfie neemt in de zaal waar de servers van de klant staan.

Er zijn ook spelletjes op de markt die helpen bij het sensibiliseren: de Serious Games[37]. Deze games simuleren allerlei aanvallen waarmee het bedrijf zijn reactievermogen kan testen en zijn beveiligingsproblemen kan onderzoeken. Doelgroep van deze games zijn voornamelijk bedrijfsleiders.

Bij het aanwerven kan men ook wijzen op het belang van veiligheid. "*Waarom bij ondertekening van het contract geen Cyber Security Policy opnemen in het arbeidsreglement?* "verklaart Jean-Marc André, oprichter van UNIWAN. "*Zo begrijpt de werknemer van bij het begin dat de onderneming veiligheid hoog in het vaandel draagt*" vervolgt hij.

De veiligheid betreft ook en vooral de bedrijven die deel uitmaken van de kritieke sectoren: energie, mobiliteit, telecombedrijven, geldwezen, verzekeringen, waterdistributie, publieke gezondheid, de overheid. In deze vitale sectoren moet men bijzondere aandacht besteden aan de veiligheid.



Figuur 5 - Belang van de computerbeveiliging Studie UCM

3.2.2 Kmo's en microbedrijven

Volgens een onderzoek van het UCM met meer dan 300 Franstalige kmo's, beweren 88% van de ondervraagde kmo's veel belang te hechten aan de informatiebeveiliging van hun onderneming.

Bovendien verklaart 51% dat ze reeds geconfronteerd werden met problemen inzake Cyberveiligheid (gegevensverlies, gehackte berichten, versleutelde gegevens, tijdelijk stilliggen, computersysteem aangevallen, etc.). 62,3% van de ondervraagden verklaart dat het veiligheidsbeheer door de baas wordt verzorgd, of door een externe persoon (bijvoorbeeld een consultancybedrijf). Ook interessant om weten is dat 1,6% beweert geen beveiliging nodig te hebben.

Wat verwacht het publiek eigenlijk? We kunnen de verwachtingen in drie prioriteiten onderverdelen: betere weerstand tegen hacking, daling van de aankoopkosten van sommige tools, en korting/fiscale aftrek op de investeringen van beveiliging van de computerinfrastructuur. 45,8% zou graag een opleiding van goede praktijken volgen.

De studie eindigt met aanbevelingen aan de overheid:
- *Meer investeren in Cyberveiligheid en de politiediensten ondersteunen in de verwerking van klachten op dit gebied;*
- *De contactpersonen en bestaande hulpmiddelen bekender maken;*

36. https://en.wikipedia.org/wiki/Red_team
37. Bijvoorbeeld: https://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html of http://www.cigref.fr/sensibiliser-a-la-cybersecurite-le-serious-game-cigref-dans-les-entreprises
38. https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiYqY6b-_TWAhXFh7QKHU1MCEYQFggmMAA&url=https%3A%2F%2Fwww.ucm.be%2Fcontent%2Fdownload%2F159663%2F3003014%2Ffile%2FUCM-ECO-%2520Cybersecurite.pdf&usg=AOvVaw1Ty17hYul79dZNns8s31I

- *Sensibiliseren inzake goed gebruik via aangepaste communicatiemethoden;*
- *Aangepaste opleidingen ontwikkelen die gericht zijn op de problemen waar kmo's mee geconfronteerd worden;*
- *Consultancy inzake informatiebeveiliging opnemen in de hulpmiddelen;*
- *Bekendmaken welke fiscale federale stimulans men kan krijgen voor investeringen in informatiebeveiliging en, de systemen voor gegevensopslag die afgestemd zijn op zelfstandigen of kmo's*[39] *…*

Het is echter algemeen bekend dat kmo's en microbedrijven zich het minst betrokken voelen bij computerbeveiliging. *"Wat de kmo's betreft moet men de zaakvoerders sensibiliseren. Vooral geen schrik aanjagen want dat lost niets op, we moeten de communicatie aanpassen aan de managers"* verklaart Grégorio Matias van MCG. Eerst en vooral moet de onderneming haar veiligheid evalueren en zich daarbij de volgende vragen stellen:
- Wat heb ik in mijn bezit? Wat produceer ik dat een risico vormt?
- Verwerk ik persoonlijke gegevens?
- Verwerk ik gevoelige gegevens?

Op basis van deze vragen kan de onderneming beslissen om een veiligheidsstrategie in te voeren die aangepast is aan de realiteit.

Volgens de heer Ferdinand Casier is het wel een *"kwestie van juiste verhoudingen. Bepaalde microbedrijven hebben niet per se een arsenaal aan beveiliging nodig"*.

En toch zijn, volgens de heer Valery Geeten, Legal Officer bij het Centrum voor Cyberveiligheid België, "*kmo's steeds vaker het doelwit van aanvallen*". Deze verandering is al een tijdje aan de gang. Vroeger richtten de hackers hun pijlen op de grote bedrijven die inmiddels over de menselijke, financiële en technologische middelen beschikken om zich te wapenen tegen cyberaanvallen. Dit geldt niet voor alle kmo's. Ze beschikken niet over dezelfde middelen en zijn zich ook niet zo bewust van het fenomeen van hacking[40]. Het gebeurt zelfs regelmatig dat hackers databanken van ondernemingen bezoeken zonder sporen na te laten.

Volgens de heer Vincent Defrenne van NVISO "*beschikken de kmo's zelden over de kritische massa en competenties om het hoofd te bieden aan deze problemen*". Kmo's zitten met drie fundamentele problemen:

- Enorme **fragmentatie** over het Belgische grondgebied: het is moeilijk om alle ondernemingen te bereiken,
- **Recurrentie**: alle kmo's reageren anders als het over Cyberveiligheid gaat. Worden ze getroffen door een probleem van Cyberveiligheid dan zoeken ze wel een oplossing, maar ze handelen niet preventief,
- Onvoldoende **maturiteit**: kmo's begrijpen de oplossingen niet die men voorstelt inzake Cyberveiligheid.

We moeten de communicatie naar de kleine(re) ondernemingen dus aanpassen. Vaak is de Cyberveiligheid binnen dergelijke onderneming geen prioriteit. Volgens de heer Nicolas Vautrin, Industrial Research and Innovation Team Leader bij Innoviris, "*beschikken de meeste kleine ondernemingen niet over de middelen om een Cyberveiligheidsexpert aan te nemen*". Dit geldt ook voor startups die hun project zo snel mogelijk van de grond willen krijgen. De veiligheid is de laatste stap, en die wordt vaak verwaarloosd. Daarom is het zo belangrijk

39. http://www.ucm.be/Defense-et-representation/Espace-presse/Espace-Presse/2017/La-cybersecurite-un-enjeu-aussi-pour-les-PME
40. Hacking : zie woordenlijst

dat de overheid kmo's begeleidt en sensibiliseert. Eens de zaakvoerders bewust zijn gemaakt van de veiligheidsproblemen is de eerste stap gezet. Daarna moeten ze een veiligheidsbeleid invoeren dat ze in hun onderneming kunnen toepassen. Te algemene tips werken niet bij dit publiek en momenteel werpt de sensibilisering weinig vruchten af. De communicatie moet gepersonaliseerd worden en het belang van beveiliging moet aangetoond worden met concrete voorbeelden.

Voor deze kleine ondernemingen kan het aanwerven van een profiel met meer algemene kennis een oplossing bieden (bijvoorbeeld: een netwerkbeheerder) die een korte opleiding rond veiligheid kan volgen. Een andere oplossing: Vaak doen deze ondernemingen een beroep op externe bronnen om de veiligheid van de infrastructuur te garanderen. Ze nemen meestal een consultancybedrijf onder de arm die hen diensten voorstelt die aangepast zijn aan de behoeften van de onderneming. Belangrijk om op te merken is dat ook deze consultancybedrijven hun kennis inzake Cyberveiligheid moeten bijschaven. De sensibiliseringscampagnes moeten dus ook op deze spelers gericht zijn.

3.3 De rol van de media

De media kunnen een belangrijke opvoedkundige rol spelen in de sensibilisering. De grootste cyberdreigingen komen steeds vaker in de media. Er gaat geen week voorbij zonder dat een nieuw virus, ransomware of ander soort cyberaanval de krantenkoppen haalt. En als deze aanvallen een grote onderneming of instelling treffen, worden ze nog meer gemediatiseerd. We moeten toch voorzichtig blijven met de rol van de pers. "*In de meeste gevallen zullen de media een gebeurtenis uitvergroten zonder ze te verklaren*" vertelt Grégorio Matias. De media spelen met het gevoel van angst omdat dat nu eenmaal makkelijker verkoopt. Grégorio Matias benadrukt dat "*men het fenomeen niet bespreekbaar maakt door mensen angst in te boezemen, maar dat angst helaas vaak wel de voedingsbodem is van de pers*". Zo komt er geen beterschap. Men moet het grote publiek sensibiliseren met uitleg en opvoeding, niet met angst.

3.4 Opleiding binnen bedrijven: een oplossing?

We hebben gemerkt dat het publiek sensibiliseren geen makkelijke zaak is. In die zin zijn opleidingen wel een goede manier om de informatie te verspreiden. De opleiding kan aangepast worden aan de verschillende profielen en behoeften.

Er zijn bedrijven die intern opleidingen organiseren om het management en de werknemers te sensibiliseren. Deze opleidingen kunnen worden gegeven door het IT-team van het bedrijf of door een extern agentschap dat gespecialiseerd is in veiligheidsopleiding.

Het is ook belangrijk om de allerjongsten bewust te maken van informatiebeveiliging. Tegenwoordig bestaan er echter weinig sensibiliseringscampagnes voor kinderen. Een kind dat zich bewust is van veilig internetten wordt waarschijnlijk een volwassene werknemer die van nature de basisveiligheidsmaatregelen toepast. Waarom wachten met sensibiliseringslessen op school in onze constant veranderende wereld waar de informatica steeds sneller evolueert,? Er bestaan nochtans initiatieven zoals dat van Child Focus, Clicksafe[41], dat advies verstrekt en tal van pedagogische[42] hulpmiddelen verleent aan professionals en ouders. Deze initiatieven zijn echter schaars en onvoldoende gekend.

41. http://www.childfocus.be/sites/default/files/manual_uploads/fiche_p_1_e-safety_pour_professionnel2_nl2.pdf
42. http://www.childfocus.be/nl/preventie/clicksafe-veilig-internetten

4 De beroepen in Cyberveiligheid

4.1 Probleem van vraag en aanbod

Zo'n tiental jaar geleden waren de beroepsprofielen in Cyberveiligheid niet zo belangrijk als nu. Sinds enkele jaren stellen we een stijging vast in de aanwervingen. De Cybersecurity beroepen zijn in volle opmars. Deze ommekeer wordt door meerdere factoren beïnvloed:
- Grote aanvallen komen in de media,
- De groeiende behoefte aan Cyberveiligheid binnen bedrijven,
- De invoering van Europese maatregelen die - tot op heden onbestaande – bedrijven ertoe aanzet de beveiliging binnen hun bedrijf te structuren.

Actuele studies geven aan dat België tegen 2020 met een tekort van 2000 experten in Cyberveiligheid[43] zal kampen. In de zomer van 2017 heeft Defensie verklaard de Cyberveiligheid verder te ontwikkelen door tegen het einde van het jaar 200 experten aan te werven[44]. De Brusselse actoren zoals het CIBG willen zelfs meerdere CISO (*Chief Information Security Officer*) aanwerven om zich voor te bereiden voor de komst van GDPR (General Data Protection Regulation). De vaststelling is frappant: er is een kloof tussen het aanbod van beroepsprofielen op de arbeidsmarkt en de vacatures van de Brusselse ondernemingen.

Nous ne pouvons pas prédire l'avenir, mais il est clair que les métiers de la Cybersécurité revêtent aujourd'hui une importance stratégique pour les entreprises et les appareils de l'état. Les besoins de recrutement actuels sont dopés par la mise en place de mesures européennes telles que le GDPR ou la directive NIS (*Network and Information Security*) que nous allons expliquer dans un point suivant (voir 4.4.1 Network and Information Security - NIS).

4.2 De indicatoren bepalen van de beroepen in Cyberveiligheid

De beroepsprofielen die geassocieerd worden met Cyberveiligheid zijn divers en gevarieerd. Zoals in veel informaticagebieden zijn functiebeschrijvingen vaak vaag.

In België bestaan er momenteel geen referentielijsten die de beroepen in informatiebeveiliging klasseren, en waar iedereen mee akkoord gaat. Bijgevolg is het nog niet helemaal duidelijk waar deze beroepen voor staan.

Tijdens de voorbereiding van dit rapport hebben we meerdere aanwervingssites bezocht om de beschrijvingen van de beroepsprofielen te analyseren; Actiris[45], LinkedIn[46], Selor[47], ICTJOB[48], etc. We hebben meerdere vacatures zowel in de privé- als in de publieke sector bestudeerd.

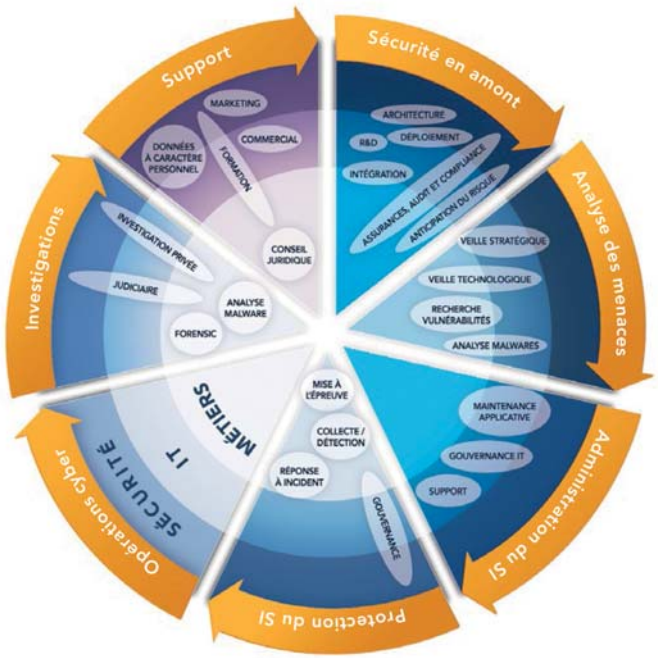
Wat kunnen we zeggen over de profielbeschrijvingen die we tijdens onze opzoekingen zijn tegengekomen? Eerst en vooral dat er danig veel functietitels zijn dat het verwarrend wordt.

43. https://www.digitalwallonia.be/centre-cybersecurite-thales/
44. http://datanews.levif.be/ict/actualite/la-belgique-va-se-doter-d-une-armee-de-200-cyberexperts/article-normal-713425.html?utm_source=Newsletter-29/08/2017&utm_medium=Email&utm_campaign=Newsletter-RNBDATANFR&&M_BT=19546149733734
45. http://www.actiris.be/ce/tabid/93/language/nl-BE/Vacatures.aspx
46. https://www.linkedin.com/uas/login
47. http://www.selor.be/nl/
48. https://www.ictjob.be/nl/?cid=SEAdvert_Google_Search_FR_Brand-BE-FR_c_B02.01%29-Exact_ictjob_FP_-_&gclid=CjwKCAjw2s_MBRA5EiwAmWIac7z003YF2Djd0aWQ39MZcRzkec_ixft7jC7lUslFhrc5Yr53GmiimhoCmu8QAvD_BwE

Cybersecurity Experts, Information Security Expert, Data Protection Officer (DPO), Information Security Risk, Information Management Consultant, Incident Response Specialist, IT Project Security Architect, Security Officer, Cybersecurity Strategy Specialist, etc. Er zijn veel te veel benamingen voor de functies in Cyberveiligheid.

In 2014 heeft een Franse studie van de CEIS[49] (Compagnie Européenne d'Intelligence Stratégique) de belangrijkste elementen voor functies in Cyberveiligheid vastgelegd.

- **De dichtheid van IT** : hieronder valt de techniciteit van het beroep (het pure IT-aspect) wat duidelijk de belangrijkste dichtheid is. Dit omvat de observatie, de ondersteuning, het onderhoud, etc.
- **De dichtheid van veiligheid** : de veiligheidscultuur met het marketingaspect, risicobeheer, etc.
- **De dichtheid van beroep** : de kennis van het toepassingsgebied en de werkomgeving. Hieronder vallen elementen zoals het juridische aspect, de compliance , het opsporen van kwetsbaarheden.



Figuur 6 - Referentiesysteem van Beroepen volgens hun dichtheid
Bron: welk referentiesysteem voor de beroepen in Cyberveiligheid?

Als we deze referentielijsten bekijken dan kunnen we enkele sleutelwoorden aanduiden die we bij voorkeur associëren aan de beroepen in Cyberveiligheid:

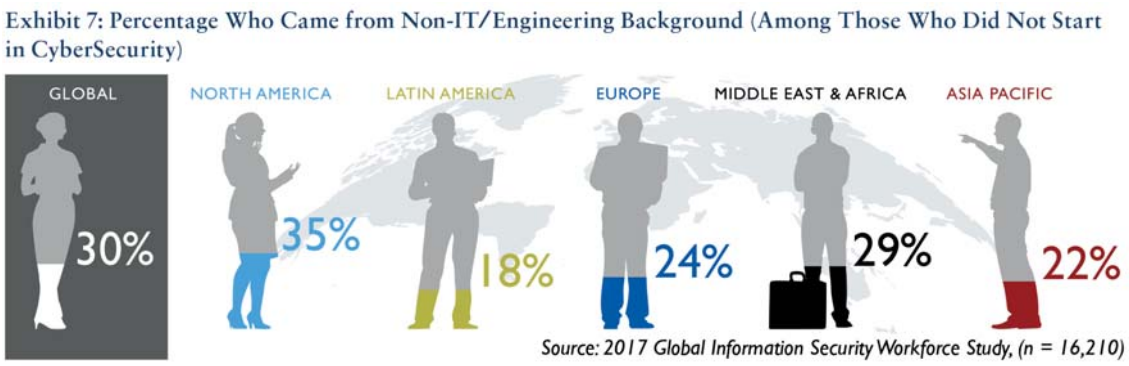
1. Communicatie (voorafgegaan door observatie),
2. Strategie,
3. Risicoanalyse,
4. Wettelijk kader.

49. https://ceis.eu/fr/accueil/
50. https://www.observatoire-fic.com/wp-content/uploads/2015/01/Policy_paper_Referentiel_metiers_-cybersecurite_CEIS.pdf
51. Compliance : zie woordenlijst.

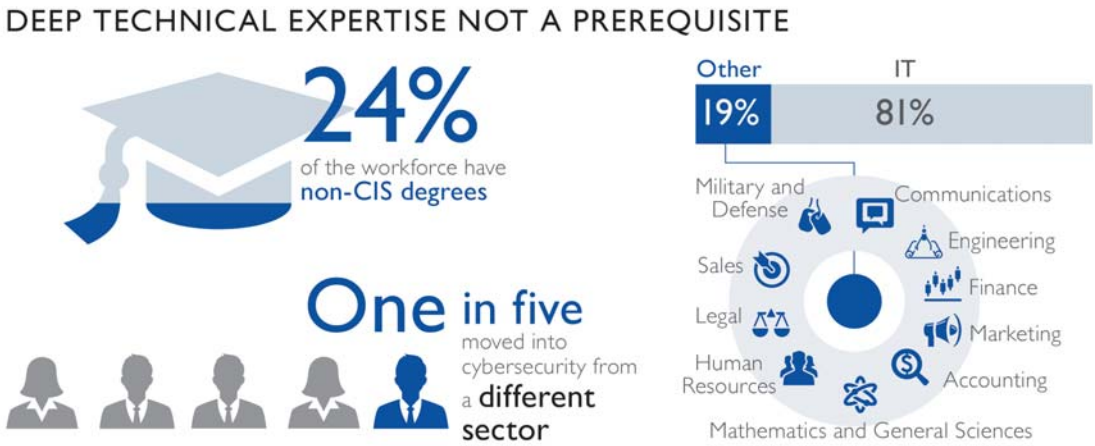
4.3 Frost & Sullivan: studie van de beroepen wereldwijd

In een studie van Frost & Sullivan[52] wordt geanalyseerd hoe het beroep van cyberspecialist er wereldwijd uitziet. De studie stelt een groeiende kloof vast tussen de stijgende virtuele bedreigingen en de aanwerving van werknemers in Cyberveiligheid. In Europa zijn slechts 66% van de functies ingevuld. De voornaamste oorzaken van dit aanwervingsprobleem zijn de moeilijkheid om gekwalificeerde mensen te vinden (48%), het feit dat de directie het veiligheidsprobleem onvoldoende begrijpt (41%), het tekort aan budget voor de aanwerving van een extra personeelslid (39%), etc. De studie benadrukt dat Europa toch 20% meer wil aanwerven.

De studie van Frost & Sullivan bekijkt ook de achtergrond van de professionals in Cyberveiligheid. Aan de hand van de cijfers stellen we vast dat 24% van de Europese specialisten een verschillend parcours hebben afgelegd en niet noodzakelijk een link hadden met IT of engineering (wat de klassieke richtingen zijn voor een functie in veiligheid). Deze 24% komt voornamelijk uit de business, marketing, financiële of militaire sector.



Figuur 7 - Profielen uit niet-IT richtingen
Bron: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf



52. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

4.4 De impact van Europese voorschriften op de beroepen

De komst van nieuwe Europese voorschriften om de Cyberveiligheid te reglementeren begint zijn invloed te doen gelden op de IT-beroepen en de manier van aanwerven. De nood om de beveiliging van gegevens en infrastructuur een wettelijk kader te geven laat zich steeds meer voelen.

Tot op heden bestaat er eigenlijk slechts één voorschrift. Dat is de richtlijn inzake "*privacy*". Ze werd ingevoerd in 1998 en bepaalt de regels voor de overdracht van gegevens binnen de Europese Unie en de Verenigde Staten.

Er bestaan wel andere maatregelen die meer gericht zijn op het beheer van persoonsgegevens en de Cyberveiligheid die we verder in dit rapport zullen voorstellen. Het betreft twee Europese maatregelen die een directe impact hebben op de kwestie van Cyberveiligheid: de NIS-richtlijn en de GDPR.

4.4.1 Network and Information Security - NIS

De richtlijn "*Network and Information Security*" is van kracht geworden in juli 2016. Met deze richtlijn wil men een "*hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Europese Unie*"[53] garanderen. Deze maatregel gaat over het algemeen gepaard met het reglement inzake gegevensbescherming (GDPR) dat we hierna zullen voorstellen.

Deze maatregel heeft gevolgen voor België[54] op twee vlakken :

1. Een nieuwe nationale Cybersecuritystrategie bepalen en een reglementair kader invoeren,
2. Het Centrum voor Cyberveiligheid[55] oprichten die de bevoegde nationale autoriteit is.

De NIS-richtlijn is enkel van toepassing op bepaalde bedrijven.

1. De dienstenleveranciers in bepaalde sectoren: energie, bank, gezondheid, digitale infrastructuur, transport, etc. …
2. De aanbieders van digitale diensten.

4.4.2 General Data Protection Regulation - GDPR

De GDRP, *General Data Protection Regulation* is een Europese wet die de regels voor gegevensbescherming bepaalt. Deze wet heeft een impact op alle bedrijven die gegevens verwerken en opslaan. Het spreekt dus voor zich dat, in tegenstelling tot de NIS-richtlijn, deze maatregel bijna alle bedrijven treft.

Art. 16, §4 van de wet van 8 december 1992

De GDPR kan beschouwd worden als de voortzetting van de wet van 8 december 1992 die het volgende stelt:

"Om de veiligheid van de persoonsgegevens te waarborgen, moeten de verantwoordelijke van de verwerking, en in voorkomend geval zijn vertegenwoordiger in België, alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens[56]".

« *Deze maatregelen moeten een geschikt veiligheidsniveau garanderen, rekening houdend met:*

1. De stand van de techniek op dit gebied,

53. http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2013/0027(COD)
54. http://www.1819.be/nl/blog/europese-richtlijn-cyberveiligheid-impact-voor-bedrijven
55. http://www.ccb.belgium.be/nl
56. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992120832&table_name=loi

2. De uitvoeringskosten van deze maatregelen,
3. De aard van de te beschermen gegevens,
4. De mogelijke risico's […][57] »

In grote lijnen zijn dit de verplichtingen van de GDPR[58]:
1. Een afgevaardigde benoemen voor de gegevensbescherming (DPO),
2. Een verhoogd veiligheidsbeleid invoeren,
3. De impact analyseren,
4. Een register maken van de verwerkingsactiviteiten.

Deze maatregel zal vanaf 25 mei 2018 van kracht worden en voorziet in tal van sancties als ze niet correct wordt toegepast.

De GDPR is de voornaamste reden waarom zoveel mensen worden aangeworven met een beroepsprofiel dat dicht aanleunt bij dat van DPO (Data Protection Officer). De deadline voor de uitvoering van de GDPR nadert met rasse schreden en heeft dus een invloed op het stijgend aantal aanwervingen in de bedrijven.

4.5 Imagoprobleem en probleem met gemengd karakter aan de kern van het probleem

De beroepen in de Cyberveiligheid hebben een nogal stereotiep imago. Als we denken aan iemand die in Cyberveiligheid werkt, dan denken we meestal onmiddellijk aan een "geek" met muffe kap op het hoofd, ergens opgesloten in een donker kamertje vol schermen. Hij tokkelt neurotisch op het toetsenbord om het computersysteem van een groot bedrijf te hacken. De pers blijft dit hardnekkige cliché hanteren waardoor de job niet aantrekkelijk lijkt. Bovendien worden sommige beroepsprofielen zoals de Pentester[59] (we verduidelijken dit profiel in deel "4.7 Focus op drie beroepsprofielen in Cyberveiligheid") momenteel als illegaal beschouwd in België. In werkelijkheid zijn de Cybersecurity profielen erg gegeerd op de arbeidsmarkt en vereisen ze ook bijzondere *soft skills*:

- Zin hebben voor communicatie en opvoeding,
- Creatief zijn en intuïtief werken
- Erg sterk zijn in opzoeken,
- Leergierig zijn,
- Zin hebben voor spel en uitdaging.

In het artikel "*The war on talent in Cybersecurity*[60]", bevestigt Koen Maris, Chief Technology Officer Cyber Security bij Atos Benelux & The Nordics, dat "*Cyberveiligheid een mindset is, geen opleiding*". De technische vaardigheden en computerskills zijn één zaak, maar om cybersecurityexpert te worden moet men ook over bovengenoemde capaciteiten beschikken, wat niet geldt voor alle informatici.

Een studie van Frost en Sullivan toont aan dat het percentage vrouwen[61] in veiligheidsfuncties behoorlijk laag is. 7% in Europa, 14% in Noord-Amerika, 9% in Afrika en 10% in Azië[62].

57. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992120832&table_name=loi
58. https://nl.wikipedia.org/wiki/Penetratietest en http://economie.fgov.be/nl/binaries/GDPR-et-NIS-quelles-obligations-de-securite-CRIDS-Dumortier_tcm325-280115.pdf
59. Penetration tester
60. http://datanews.levif.be/ict/actualite/la-guerre-des-talents-en-cybersecurite/article-opinion-656407.html
61. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf
62. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

Deze cijfers stijgen nauwelijks en dat is een probleem aangezien 50% van de vrouwen die in Cyberveiligheid werden aangeworven een hoger diploma dan een master hebben, wat meer is dan de 45% bij de mannen[63]. Bij de vrouwen zien we wel een eerder atypisch parcours in tegenstelling tot zij die over het algemeen uit de klassieke richtingen komen (zoals informatica, ingenieurswetenschappen, et.). Toch onderscheiden sommige beroepsprofielen, zoals dat van de pentester, zich van de algemene statistieken. We analyseren het profiel van de pentester in deel 4.7 Focus op drie beroepsprofielen in Cyberveiligheid.

Een interessant voorbeeld in verband met de problematiek rond het gemengde karakter is het Cyber Wayfinder -project. Dit initiatief richt zich tot vrouwen die in Cybersecurity willen werken. Het doel van Cyber Wayfinder[64] is om een Belgische gemeenschap van vrouwelijke Cybersecurityexperten op te zetten en een netwerk van bedrijven op te richten die gekwalificeerde profielen zoeken. Dit programma concentreert zich rond een aantal Bootcamps en lessenreeksen die in Brussel worden georganiseerd door de codeerschool Le Wagon[65].

4.6 Aanwervingsmethoden: Nood aan evolutie?

België kampt met een tekort aan Cybersecurityexperten, zoveel is zeker. Ondanks de talrijke nieuwe opleidingen wordt nog steeds niet voldaan aan de vraag naar experten. Veel specialisten zijn afkomstig uit het buitenland want ze zijn hoger opgeleid en talrijker, zo eenvoudig is het.

De problematiek rond de aanwezigheid van een securityexpert doet nadenken over de manier waarop wordt aangeworven. In 2017 stelt het verslag van Frost & Sullivan[66] dat, gezien de kenmerken van de Cybersecurityberoepen (te weinig vrouwen, profielen uit andere achtergronden dan IT), de manier van aanwerven moet veranderen. Het rapport stelt voor om meer afstand te nemen van het criterium van de beroepservaring gezien het stijgend aantal werknemers uit niet traditionele gebieden die zich snel aanpassen aan de vaardigheden en de vereisten van het beroep. We mogen het belang van de soft skills in dit beroep niet vergeten. De huidige manier van aanwerven creëert barrières terwijl de beroepswereld zoveel vacatures in te vullen heeft.

Bij veel bedrijven staat veiligheid niet bovenaan de prioriteitenlijst en hebben ze niet de financiële middelen om hiervoor een nieuwe werknemer aan te nemen. Zelfs als de bedrijven veiligheidsmaatregelen moeten invoeren vinden ze het zelden nodig een expert aan te werven. Er zijn ook andere mogelijkheden: een personeelslid omvormen tot securityexpert of een beroep doen op consultancybedrijven die gespecialiseerd zijn in Cybersecurity.

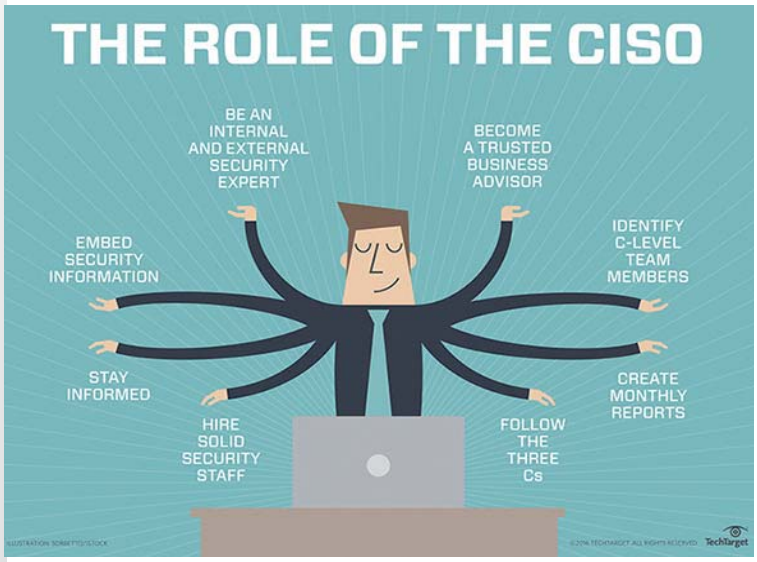
Hoe dan ook, de vacatures worden steeds talrijker en zijn vaak afkomstig van grote ondernemingen of gouvernementele organisaties. De andere bedrijven scholen een of meerdere werknemers (vaak informatici) om, of beslissen om een beroep te doen op externe consultancy.

4.7 Focus op drie beroepsprofielen in Cybersecurity

4.7.1 De CISO

De *Chief Information Security Officer* (CISO) is strikt genomen de EXPERT in beveiliging. Hij wordt vaak genoemd in de debatten over Cybersecurity en helpt zijn bedrijf het

63. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf
64. https://www.linkedin.com/company/17997439/
65. https://www.lewagon.com/fr/brussels ==> https://www.lewagon.com/brussels
66. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf



Figuur 8 - De rol van de CISO

bron: Search Security: http://searchsecurity.techtarget.com/definition /CISO-chief-information-security-officer

vooropgestelde veiligheidsniveau te bereiken en te behouden[67]. Hij is de sleutelfiguur die optreedt bij computeraanvallen maar het is ook zijn taak om een preventieve strategie in te voeren om problemen te vermijden. Hij ziet erop toe dat de netwerken en infrastructuren voldoende beveiligd zijn. In de hiërarchie van het bedrijf zit dit profiel tussen het management en de werknemers. Hij is ook de tussenpersoon voor alle veiligheidsgerelateerde vragen. Hij stelt technische adviezen op (een firewall installeren, updates, etc.) en bepaalt de good practices met als doelstelling het inbouwen van een duurzame veiligheidscultuur binnen het bedrijf. Hij heeft dus een goede kennis van beveiliging, netwerkadministratie (hij moet de norm ISO 27000 beheersen), maar ook van *Risk Management* (risicobeheer). Hij moet met de directie kunnen communiceren maar ook met de werknemers of klanten. Hij moet ook een goed inzicht hebben in het juridische kader en de veiligheidsmaatregelen van zijn beroep.

Hij houdt zich in hoofdzaak bezig met het oplossen van veiligheidsproblemen binnen het bedrijf. Hij spendeert veel tijd aan communiceren met zijn collega's en het herinneren aan de veiligheidsvoorschriften. Hij zorgt ervoor dat zijn bedrijf aan de voorwaarden voldoet om de verschillende regels en Europese maatregelen na te leven. "*Hij vervult de rol van strateeg, communicatiespecialist, expert, influencer en manager*". Deze zin, afkomstig van de site SPSearch Promoteur de talents[68], vat heel goed samen hoe complex de functie *Chief Information Security Officer* is. Voor deze functie zijn drie eigenschappen vereist: autoriteit, zelfstandigheid en verantwoordelijkheid[69].

De CISO is meestal een academicus. Hij heeft informatica en ingenieurswetenschappen gestudeerd en zich gespecialiseerd in beveiliging. Gezien zijn functie van expert en zijn strategische rol binnen het bedrijf is een zekere ervaring op het gebied van beveiliging vereist. Voor die reden zoekt men in de meeste vacatures voor deze functie naar een hoog opgeleid profiel met meerdere jaren ervaring in het vakgebied.

We komen dit beroep over het algemeen tegen in grote ondernemingen of organisaties die over de middelen beschikken (financiële en menselijke middelen en strategische prioriteit) om een CISO aan te werven. In de kleinere ondernemingen is het veelal een beheerder van het informaticapark die de functie van *Meneer Security* op zich neemt. In ondernemingen zoals kmo's[70] wordt de functie vooral geoutsourcet. Deze ondernemingen doen een beroep op consultancy bedrijven die het informaticapark van het bedrijf met al zijn veiligheidsaspecten beheren.

67. https://fr.wikipedia.org/wiki/Responsable_de_la_s%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information
68. http://spsearch.fr/blog/cest-quoi-un-expert-de-la-cyber-securite/ ⇒ http://spsearch.fr/en/blog/what-is-an-expert-in-cyber-security/
69. https://www.linkedin.com/pulse/can-ciso-act-dpo-georges-ataya?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_search_srp_content%3Baz6G7KX2d7AmzdAb%2FgIHdg%3D%3D
70. https://www.ysosecure.com/securite-information/role-rssi.html

TECHNISCHE VAARDIGHEDEN DIE OVER HET ALGEMEEN VEREIST ZIJN VOOR EEN CISO

- CompTIA Security+,
- GSEC: GIAC Security Essentials Certification,
- SSCP: Systems Security Certified Practitioner,
- CISSP: Certified Information Systems Security Professional (certificaat informatiebeveiliging),
- CISA: Certified Information Systems Auditor in het bijzonder voor auditors,
- CISM: Certified Information Security Manager, gericht op management bijvoorbeeld voor de CIO,
- GCIH: GIAC Certified Incident Handler (voor de incidentenbeheerder; alles wat te maken heeft met het opsporen en beheren van beveiligingsincidenten),
- CEH: Certified Ethical Hacker,
- OSCP: Offensive Security Certified Professional,
- IT-strategie, architectuur en bedrijfsveiligheid,
- Veiligheidsconcepten rond DNS, routing, authenticatie van gebruikers en toestellen, VPN, proxydiensten en DDOS technologie,
- ISO 27002, ITIL en COBIT- framework,
- De compliance- checklists (homologatie) PCI, HIPAA, NIST, GLBA en SOX,
- Windows, Unix en Linux besturingssysteem,
- C, C++, C#, Java en/of PHP,
- Protocollen firewall en detectie/preventie van indringing,
- Ervaring in veilig coderen, ethisch hacken en in kaart brengen van TCP/IP bedreigingen, netwerk, routing en switching,
- Ontwikkeling en definitie van architectuur netwerkbeveiliging,
- Kennis van hulpmiddelen en methodes voor de audit, en van Cloud-gerelateerde risico-evaluatie.

4.7.2 De DPO

De Data Protection Officer is de "*conformiteitsdirigent*[71]". Dit beroepsprofiel is ontstaan door de GDPR maatregel die de aanwezigheid van een DPO in alle administraties verplicht maakt.

Wie is de DPO? Hij valoriseert de gegevens en stelt de gebruiksregels op. Het bedrijf kan iemand aanwerven voor de functie van DPO, een werknemer benoemen tot DPO of een beroep doen op een externe consultant als DPO.

In tegenstelling tot de CISO hoeft de DPO niet noodzakelijk expert te zijn in Cybersecurity. Hij moet wel over een degelijke juridische kennis en informaticakennis beschikken[72]. Hij moet een goede projectmanager zijn en goed kunnen communiceren. Hij moet ervoor zorgen dat de preventieve beveiligingsmaatregelen worden nageleefd maar hij is ook de persoon die snel moet ingrijpen in crisissituaties.

71. 72. Le métier de Data Protection Officer (DPO), obligatoire dès 2018 dans de nombreuses entreprises, Blog du Modérateur [en ligne] http://www.e-marketing.fr/Thematique/general-1080/Breves/Fiche-metier-data-protection-officer-313562.htm#30HLowl0ppDV6UR6.97
73. Privacy by design : zie woordenlijst.

Figuur 9 - het beroep van Data Protection Officer bron afbeelding http://www.abilways-digital.com

De DPO zorgt dat het concept "*Privacy by design*[73]" wordt toegepast. Dit concept integreert de gegevensbescherming vanaf het ogenblik dat het informatiesysteem of –netwerk is ontworpen en werkt. Hij is ook verantwoordelijk voor de sensibilisering en werkt hiervoor een gids uit met goede praktijken om in alle veiligheid te werken. Hij is dé sleutelfiguur om aan te spreken voor alles wat met persoonsgegevensbescherming te maken heeft.

Hij werkt samen met de CISO en de directie. Hij is een tussenpersoon voor de werknemers en communiceert welke veiligheidsmaatregelen moeten getroffen worden.

Over het algemeen beschikt de DPO over een master in informatica, maar dit is geen vereiste. Hij volgde vaak aanvullende opleidingen of behaalde certificaten (voorbeelden van DPO-opleidingen in het hoofdstuk over de opleiding) voor de functie van afgevaardigde van gegevensbescherming.

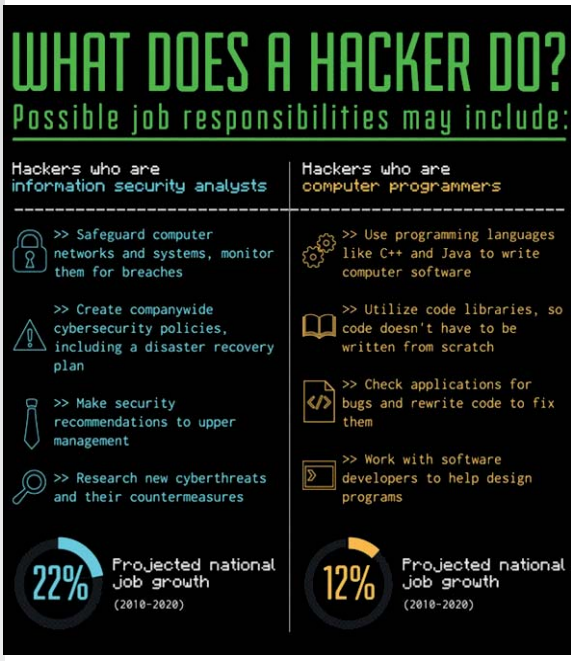


Figure 10 - What does a hacker do?
https://fossbytes.com/how-to-become-a-ethical-hacker/

4.7.3 De "ethische hacker"

De ethische hacker is de informatie-veiligheidsonderzoeker die samenwerkt met organisaties (privébedrijven, vzw's of overheidsinstellingen) om kwetsbaarheden op te sporen in hun informatiesystemen of -netwerken. Met toestemming van de betrokken organisatie stelt hij zich in de plaats van een hacker en test de informatiesystemen van de organisatie. Hij is verplicht om het beleid inzake de gecoördineerde bekendmaking van kwetsbaarheden na te leven (in het Engels "coordinated vulnerability disclosure policy") of een beloningsprogramma voor kwetsbaarheden (in het Engels "vulnerability rewards program" of "bug bounty program") van de organisatie die verantwoordelijk is voor het informatie-systeem.

Volgens de definitie van het CCB is een beleid van gecoördineerde bekendmaking (of "beleid van verantwoorde bekendmaking") van kwetsbaarheden een verzameling regels die vooraf door een ICT-organisatie werd bepaald en die toestemming geeft aan veiligheidsonderzoekers of aan het grote publiek om met goede intenties mogelijke kwetsbaarheden op te sporen in hun systemen, of om relevante ontdekte informatie hieromtrent te bezorgen. Deze regels, die meestal openbaar zijn gemaakt op een website, leggen een juridisch kader vast voor de samenwerking tussen de verantwoordelijke organisatie en de deelnemers aan het beleid.

74. Le métier de Data Protection Officer (DPO), obligatoire dès 2018 dans de nombreuses entreprises in Blog du modérateur https://www.blogdumoderateur.com/metier-data-protection-officer-dpo/

Ook al spreekt de term expliciet over de "bekendmaking" van de kwetsbaarheden, toch is dit geen noodzakelijke voorwaarde voor een beleid van gecoördineerde bekendmaking. In werkelijkheid is dit gewoon een facultatieve module die de partijen vrij kunnen kiezen, in tegenstelling tot de toestemming die gegeven wordt om toegang te krijgen tot de systemen van de verantwoordelijke organisatie.

In dat opzicht vormt het beleid van gecoördineerde bekendmaking van kwetsbaarheden een contract waarin alle contractbepalingen werden vastgelegd door de verantwoordelijke organisatie en daarna werden aanvaard door de veiligheidsonderzoeker als hij beslist om deel te nemen aan het ingevoerde programma.

Wat het beloningsprogramma voor kwetsbaarheden betreft, dit zijn een verzameling regels die een verantwoordelijke organisatie heeft bepaald om beloningen te geven aan veiligheidsonderzoekers of het grote publiek die kwetsbaarheden in haar technologieën detecteren. Deze beloning kan een som geld zijn, cadeaus of een eenvoudige publieke erkenning.

Voor zover de wettelijke bepalingen worden nageleefd (voorwaarden voor de toestemming van de organisatie, andere strafbepalingen, het geheim van elektronische communicatie en de persoonsgegevensbescherming), is ethisch hacken perfect legaal in België.
In 2018 zou het CCB een Gids uitbrengen over het beleid van gecoördineerde bekendmaking van kwetsbaarheden in België. Deze gids zal een deel omvatten over de goede praktijken (met een beleidsmodel) en een deel over de wettelijke aspecten.

De eigenschappen van de ethische hacker zijn: nieuwsgierigheid, zelfstandigheid, de capaciteit om "out of the box[75]" te denken en zich in de plaats te stellen van een hacker. Hij spoort problemen op en stelt verbeteringen voor. Hij wordt ook "pentester" genoemd (samentrekking van "penetration tester[76]") en identificeert mogelijke toegangspunten, probeert binnen te dringen en documenteert zijn resultaten[77]. De ethische hacker heeft een goed gevoel voor spel en uitdaging. Elk project is voor hem een nieuwe gelegenheid om aan de klanten te tonen dat hun bedrijf niet onkwetsbaar is. Hij zoekt elke toegangspoort tot de infrastructuur van het bedrijf (computer of fysieke indringing) om zo de gevoeligheden van het systeem bloot te leggen en hij stelt verbeteringen voor aan de klant. (Bijvoorbeeld wat het bedrijf Digital Security doet met haar speciale audittechniek de Red Team Attack[78]). Ook al bestaat er strikt genomen nog geen opleiding voor ethisch hacken, toch nemen sommige masters het thema op in hun programma maar dan op een bewust vage manier. Men leert het beroep in aanvullende opleidingen (Certified Ethical Hacker "CEH")[79] of aan buitenlandse universiteiten. In Maubeuge in Frankrijk kan men de *licence professionnelle des collaborateur pour la défense et l'anti-intrusion des systèmes informatiques* (CDAISI)[80] volgen. Met deze opleiding wordt men "*Pentester*".

75. http://www.orange-business.com/fr/blogs/securite/securite-organisationnelle-et-humaine/conseils-pour-devenir-un-hacker-ethique-osd14
76. Penetration tester : zie woordenlijst.
77. http://www.pentesteur.com/pentesteur-ethical-hacking
78. Zie Hoofdstuk 3.2: De ondernemingen sensibiliseren 3.2.1 De grote ondernemingen.
79. Howest, Hogeschool West-Vlaanderen
80. http://www.univ-valenciennes.fr/IUT/lecole-des-hackers-maubeuge

5 Opleidingen in Cybersecurity in Brussel

In België bestaan een aantal opleidingen waar informatiebeveiliging op meerdere niveaus wordt onderwezen. Deze opleidingen zijn een antwoord op de groeiende nood aan Cybersecurityspecialisten. Er is voor elk wat wils: masters, bachelors, specialisaties, certificaten, voortgezette opleidingen, etc. In dit rapport concentreren we ons op het Brusselse landschap[81]. Het probleem nu is dat we in de meeste opleidingen geen duidelijk verband zien met de problemen op het terrein en men pedagogisch vaak de nochtans essentiële "soft skills" onderschat (of zelfs vergeet) die aan Cybersecurity gelinkt zijn. De lessen Cybersecurity vallen meestal onder de noemer informatica, ingenieurswetenschappen, management en recht.

De academische wereld begint zich bewust te worden van de nood aan Cybersecurityprofielen. In Brussel worden een aantal opleidingen ontwikkeld die hier een antwoord moeten op bieden. Goede toekomstperspectieven voor de personeelswerving dus.

Op de site van het CCB[82] is een volledige lijst beschikbaar van de opleidingen in Cybersecurity over heel België.

5.1 De universitaire opleidingen

5.1.1 Master in Cybersecurity (VUB, UCL, UNamur, ERM, HELB, ESI-HEB)[83]

De Universiteit van Namen, de Vrije Universiteit van Brussel, de Franstalige Katholieke Universiteit van Louvain-La-Neuve (UCL), de Vrije Hogeschool van Brussel, de Vrije Hogeschool Brussel-Brabant (ESI) en de Koninklijke Militaire school (ERM) hebben zich samen ingezet om deze master in het leven te roepen. De cursussen lopen over twee jaar en worden gegeven op drie campussen in Brussel, Leuven en Namen.

De domeinen die worden bestudeerd zijn de volgende:

- Cryptografie en cryptanalyse,
- Informatie- en telecommunicatienetwerken,
- Informatieveiligheid en beveiliging van informatiesystemen,
- Technieken voor beheer en verwerking van metadata, inferentie en informatielekken
- Forensische[84] wetenschap en onderzoek,
- Veiligheidsbeheer en invoering van normen, audits en veiligheidsbeleid,
- Legale, ethische en menselijke aspecten van de veiligheid,
- Ontwerp van architecturen van beveiligde systemen,
- Methodes van software engineering en beveiligde ontwikkeling.

Naast deze puur technische vaardigheden houdt deze master ook rekening met de vragen die we bij de vacatures konden vaststellen. Laten we enkele belangrijke sleutelwoorden herhalen: communicatie (voorafgegaan door observatie), strategie, risicoanalyse en juridische gelijkheid. Aangezien de veiligheidsspecialist de vaardigheden moet hebben van een informaticus, manager en informatieverstrekker, moeten deze elementen opgenomen worden in deze master, zeker als hij over twee jaar wordt gespreid.

81. Deze lijst is informatief, veranderlijk en niet exhaustief.
82. http://www.ccb.belgium.be/fr/ict-security-education-belgium
83. https://masterincybersecurity.ulb.ac.be/
84. Forensische wetenschap: zie woordenlijst

De opleiding kan worden gevolgd door houders van een bachelor in informatica of ingenieurswetenschappen, de student moet dus een informaticaprofiel hebben.

Deze cursus kan ook nuttig zijn voor informatici die hun kennis inzake veiligheid willen uitbreiden en die na enkele jaren ervaring op de werkvloer zich verder willen specialiseren.

5.1.2 Information security management education – Solvay Brussels School (VUB)[85]
Deze opleiding bestaat uit twee formules:

Eerst een master van 288 uren les die de volledige modules bevat:

1. Module **S** Information Security,
2. Module **G** Digital Governance,
3. Module **M** IT Management,
4. Module **B** Business Transformation.

Vervolgens zijn er drie personaliseerbare programma's van 144 uur les:

1. De modules S et G,
2. De modules S et B,
3. De modules S et M.

Deze opleiding is bestemd voor managers en niet voor pur sang informatici, ook al is de module inzake veiligheid automatisch opgenomen in alle programma's. Met deze module verwerft men onder andere managementvaardigheden en gedragscompetenties zoals preventie, leert men omgaan met risico's, en leert men Cybersecurity gerelateerde technologieën.

5.2 Cybersecuritylessen aan de universiteit

Er worden regelmatig lessen over Cybersecurity gegeven in de meer klassieke opleidingen (ingenieurswetenschappen, informatica, etc.) Dankzij deze integratie kunnen de toekomstig afgestudeerden de problematiek rond Cybersecurity in hun beroep begrijpen en integreren.

We zullen even enkele van deze lessen onder de loep nemen.

Protocols, cryptanalysis and mathematical cryptology - VUB. Deze cursus wordt gegeven in het programma van informatiewetenschappen of aan de burgerlijk ingenieurs informatica. Deze cursus biedt namelijk "een inleiding tot de specifieke onderzoeksmethoden in cryptologie, en integratie van de belangrijkste resultaten van moderne cryptanalyse in het design en de analyse van cryptografische primitieven en protocollen[86]».

Operating systems and security – VUB[87]. Deze cursus wordt gegeven in de faculteit ingenieurswetenschappen in het departement Elektronica en Informatica. Dankzij deze cursus voor geavanceerde technische vaardigheden kan men kennis verwerven in onder andere veiligheidsbedreigingen, "invaders", malicious software, Windows veiligheid, etc. Deze cursus is speciaal omdat hij wordt gegeven onder de vorm van een MOOC[88] met hulp op afstand.

85. http://exed.solvay.edu/fr/13-gamme/10-digital-transformation-it-education
86. http://banssbfr.ulb.ac.be/PROD_frFR/bzscrse.p_disp_course_detail?cat_term_in=201516&subj_code_in=INFO&crse_numb_in=F514&PPAGE=ESC_PROG-CAT_AREREQ&PPROGCODE=MA-IRIF&PAREA=M-IRIFS&PARETERM=201516&PTERM=201516
87. https://www.vub.ac.be/en/study/fiches/55982/operating-systems-and-security
88. MOOC: zie woordenlijst.

5.3 De hogescholen

Heel wat hogescholen geven ook Cybersecurityopleidingen of integreren cursussen hierover in een meer algemene informaticaopleiding (lijst van het CCB[89]). Deze opleidingen bestaan in de vorm van bachelor, master of volwaardige opleiding en worden steeds talrijker in de Brusselse hogescholen.

5.3.1 Bachelor specialisatie in informatienetwerken en –systemen – HEB (Hogeschool Brussel)[90]
Dit specialisatiejaar wordt gekenmerkt door een aangepast uurrooster (mogelijk om over twee jaar te spreiden) en beoogt drie doelstellingen:
1. Zelfstandig en in team kunnen werken,
2. Meegaan in het concept van veiligheidsaanpak volgens een methode,
3. De specifieke ervaring van beveiliging van informatiesystemen mobiliseren.

Dankzij dit specialisatiejaar kan de houder van een bachelor of master in informatica vaardigheden verwerven op het gebied van Cybersecurity in een specialisatiejaar.

5.4 De certificaten en voortgezette opleiding

Certificaten behalen is een prima manier om specifieke vaardigheden in een bepaald vakgebied te verkrijgen. "*Helaas zijn deze cursussen vaak privé, betalend en belachelijk duur*" vertelt Jean-Jacques Quisquater, expert in cryptografie aan de UCL.

Er bestaat ook een voortgezette opleiding in Cybersecurity. We vinden een voortgezette opleiding in Cybersecurity terug aan de UCL[91].

5.4.1 Certificaat van Data Protection Officer
Aangezien de GDPR het verplicht maakt om een DPO aan te werven is dit soort opleiding volop in opmars in Brussel. We zullen twee van die opleidingen nader bekijken.

1. 1. De Data Protection Officer Certificatie - DPInstitute[92]
Dit is een 5-daagse opleiding die voorbereidt op de functie van Data Protection Officer (DPO).

De opleiding behandelt de Europese privacy wetgeving, het werk van de DPO, risico- en privacymanagement, audit en controle, incidentenbeheer …

2. 2. Data Privacy security management – ICHEC[93]
6-daagse opleiding die net zoals de vorige opleiding dient om de nieuwe verplichtingen van de DPO aan te leren. Op het einde van de opleiding moet de student goed zijn in crisiscommunicatie, moet hij risico's inzake informatiebeveiliging kunnen identificeren, moet hij de rol en strategische functie van de DPO binnen het bedrijf begrijpen, etc.

89. http://www.ccb.belgium.be/nl/ict-security-education-belgium
90. http://www.heb.be/esi/bachelierSecu_fr.htm
91. https://uclouvain.be/fr/etudier/iufc/formation-continue-cybersecurite.html
92. https://www.dp-institute.eu/nl/opleidingen/data-protection-officer-certificatie-training/
93. https://www.ichecformationcontinue.be/fr/data-privacy-security-management.html?IDD=553648329&IDC=138

5.5 Korte opleidingen

5.5.1 Evoliris

Het bijzondere aan Evoliris is dat het een aantal opleidingen van korte duur aanbiedt. De volgende opleidingen hebben te maken met Cybersecurity.

Cyberdefensie en anti-indringing : tijdens deze 5-daagse opleiding leert men de werking van computeraanvallen begrijpen, zodat men zelf kan binnendringen in systemen en tegenmaatregelen kan uitwerken,

Beveiliging van een Windows werkstation : dekt de belangrijkste beveiligingsaspecten van een Windows werkstation in steeds meer mobiele toepassingen.

Linux beveiliging: een Linux server beveiligen en controleren.

Deze beroepsgerichte opleidingen zijn gebaseerd op de realiteit op het terrein en de behoeften van de arbeidsmarkt, zodat het voor stagiairs mogelijk wordt om in een korte tijdspanne volwaardige opleidingen te volgen.

5.5.2 Intec

ICT Security Specialist[94] : met deze opleiding, die bestemd is voor werkzoekenden met een goede kennis van het Nederlands, verwerft men vaardigheden van netwerken en servers. Men leert er ook de laatste securitytechnologieën. Verder geeft men er: beveiligen van CISCO-netwerkapparaten, authenticatie, autorisatie, accounting, CISCO-firewall technologieën implementeren, cryptografische systemen, CISCO VPN's implementeren, lokale netwerken beveiligen, beveiliging van de meest courante rollen van Windows Server (AD, DNS, DHCP, IIS, WSUS, Fileservices), Exchange, basisconfiguratie, Virtualisatie, ITIL, Firewall.

Digital Skills - Cybersecurity[95] : opleiding van twee weken waar men digitale vaardigheden in Cybersecurity leert.

5.6 Andere opleidingen

5.6.1 Cyber WayFinder

We hebben dit initiatief reeds besproken in het hoofdstuk Imagoprobleem en probleem rond gemengd karakter aan de kern van het probleem. Deze opleiding is gericht op vrouwen die in Cybersecurity willen werken en is opgebouwd rond twee assen[96] : eerst worden er Bootcamps[97] rond veiligheid georganiseerd. Daarna volgt de rest van de opleiding waar bijscholingscursussen worden gegeven met oefeningen (lessen over Risk Management, cryptografie, over de GDPR wetgeving, etc.).

5.6.2 Opleiding voor bedrijven

Sensibiliseringscursussen of technische cursussen voor het management of de werknemers; de opleidingen voor bedrijven zijn een oplossing om een veiligheidscultuur te creëren binnen bedrijven. De opleiding wordt ofwel door het bedrijf gegeven (meestal geeft de CISO deze cursus), ofwel door een externe consultant. Ze wordt gegeven in de bedrijfslokalen of via e-learning. Het CCB heeft de handen in elkaar geslagen met het OFO om opleidingen aan te

94. http://www.intecbrussel.be/Werkzoekende/WerkzoekendeHome/ICTSecuritySpecialist.aspx
95. http://www.intecbrussel.be/Werkzoekende/Opleiding/Cybersecurity(DigitalSkills).aspx
96. https://drive.google.com/file/d/0Bx3M43y7I6aYV3hPanA4aW1qNFU/view
97. Bootcamps: zie woordenlijst

bieden aan IT-managers en IT–medewerkers die op een federale overheidsdienst[98] werken. Er bestaan verschillende opleidingen van enkele dagen die op de werkplaats kunnen gegeven worden. De Solvay Brussels School biedt ook een 5-daagse opleiding aan, namelijk het "*Programme in European Data Protection*". Met deze opleiding kan met een certificaat voor het beroep van DPO[99] behalen.

5.6.3 L'e-learning

E-learning blijft een goede manier om informaticakennis bij te werken. Er bestaan ook opleidingen in Cybersecurity. Zo is er de "Eurometropolitan E-Campus[100]" met een opleiding in Cybersecurity die in 5 modules is opgesplitst. Deze opleiding is bestemd voor bedrijven en kmo's die hun personeel willen sensibiliseren inzake veiligheid. E-learning is vaak een handige oplossing om het personeel te onderrichten over de beveiligingsmaatregelen.

98. https://www.ofoifa.belgium.be/nl/cybersecurity-een-uitgebreid-opleidingsaanbod-voor-zowel-it-managers-als-it-medewerkers
99. http://exed.solvay.edu/fr/11-program/221-programme-in-european-data-protection
100. http://www.ee-campus.be/index.php/formations

Conclusie

Op enkele jaren tijd is Cybersecurity uitgegroeid tot een Europese, federale en regionale, maar ook economische en maatschappelijke uitdaging. Na afloop van dit rapport hebben we over het algemeen meerdere problemen vastgesteld:

1. Brussel is nog niet klaar om een Cybersecuritystad te worden maar haar centrale ligging in Europa biedt haar wel de mogelijkheden om het te worden.
2. In België is er een groeiende kloof tussen het aanbod van beroepsprofielen op de arbeidsmarkt en het aantal vacatures,
3. Deze kloof wordt gedeeltelijk beïnvloed door het tekort aan beschikbare kwalificerende opleidingen in België,
4. Er is het eeuwige sensibiliseringsprobleem. De oplossing zou zijn om de communicatie naar de verschillende doelgroepen (kinderen, bedrijfsleiders, werknemers, etc.) aan te passen en te versterken maar dat is een werk van lange adem dat constant herhaald moet worden zodat veiligheid een automatische reflex wordt.
5. Er bestaan geen referentielijsten van de beroepen, en de definities van hun profielen en vaardigheden zijn vaag,
6. Er is vaak een kloof tussen de opleidingen en de realiteit op het terrein,
7. De pers en de overheid kunnen een rol spelen in het overbrengen van de goede praktijken,
8. Het probleem rond het gemengd karakter is deel van het aanwervingsprobleem.

Pistes voor oplossingen en aanbevelingen

Doorheen dit rapport hebben we geprobeerd de problematiek rond Cybersecurity te schetsen aan de hand van verschillende Brusselse assen (economisch, politiek, academisch en op het niveau van beroepsprofielen). De situatie is niet eenvoudig met de sensibiliseringsproblemen (hoe kunnen we de verschillende doelgroepen bereiken en hen sensibiliseren inzake Cybersecurity?), het gebrek aan structuur op niveau van de beroepsprofielen (te veel functietitels en te vage functiebeschrijvingen), het gebrek aan maturiteit van Brussel (fragmentatie van de politieke instanties, wil tot centralisatie via het CCB, …) en de problemen inzake aanwerving (probleem rond gemengd karakter, tekort aan diverse profielen, tekort aan profielen op de Belgische arbeidsmarkt, …).

Als conclusie geven we een reeks aanbevelingen of denkpistes als aanvulling op het debat rond Cybersecurity in Brussel.

1. Brussel de positie geven van Europese Cybersecurity hoofdstad

Gezien haar strategische positie binnen Europa en in samenwerking met de Europese initiatieven moet Brussel het voorbeeld geven door een Cybersecuritystrategie toe te passen. Op dit moment kampt onze hoofdstad echter met een gebrek aan maturiteit tegenover deze problematiek.
Voorgestelde denkpistes:

- Bekendmaken van acties van organisaties die ijveren voor Cybersecurity door sterke communicatie te voeren en de informatie te centraliseren op platformen die referentietools kunnen worden.
- Wat de tewerkstelling betreft moet Brussel met haar strategische ligging de talenten en specialisten in Cybersecurity aantrekken.
- De opleidingen moeten het resultaat zijn van gemeenschappelijk overleg tussen de behoeften van de bedrijven en de opleidingsactoren.

2. Op jonge leeftijd beginnen sensibiliseren

De sensibilisering is een echte uitdaging geworden. Tot op welk punt kunnen we de mensen verplichten om goede preventiemaatregelen te hanteren? Het moeilijkst is om de mensen te bereiken die vinden dat zij geen problemen hebben met Cybersecurity. Zoals we hebben gezien is de menselijke factor meestal de zwakke schakel in de veiligheid. Een oplossing zou kunnen zijn om de burgers op zo jong mogelijke leeftijd op school of tijdens buitenschoolse activiteiten te sensibiliseren. Er bestaan nog te weinig dergelijke initiatieven in België. Als men de aanvalsproblemen kent, kan men er zich beter tegen wapenen en daarom moeten we de kinderen continu en van jongs af aan hierin opvoeden. De beste manier om de allerjongsten te bereiken is in de eerste plaats via de ouders en leerkrachten. Het zijn zij die dagelijks de goede praktijken moeten herhalen. **Toespraken op scholen** bieden pedagogisch hulpmiddelen aan leerkrachten en ouders die hun kinderen willen aanleren om veilig te internetten. We moeten de volwassenen praktische tips geven waarmee ze hun kennis kunnen overbrengen, zodat hun kinderen de basisregels onbewust toepassen. Initiatieven zoals Clicksafe van Childfocus[101] moeten verder ontwikkeld worden om bekender te worden.

3. De preventiemiddelen in ondernemingen uitbreiden

De veiligheid in ondernemingen is een terugkerende problematiek. We moeten twee soorten doelgroepen onderscheiden: het management en de werknemers. Om te beginnen is het management vaak moeilijk te bereiken. Wanneer de directie zich bewust is van de veiligheidsproblematiek is het over het algemeen gemakkelijker om een veiligheidsbeleid in te voeren. Maar de werknemers hebben ook nood aan specifieke communicatie die hen herinnert aan de basisveiligheidsregels. Het veiligheidsbeleid moet voor iedereen gelden en wordt aan de hand van meerdere aanbevelingen herhaald. Om de werknemer te bereiken moeten we hem betrekken bij de bedrijfsveiligheid. Het is over het algemeen de functie van de DPO en de CISO om de veiligheidsmaatregelen mee te delen.

Elke onderneming moet een geldig **veiligheidsbeleid** invoeren dat van toepassing is op alle bedrijfsleden. Meestal is de veiligheidsverantwoordelijke verantwoordelijk voor deze sensibilisering, hij moet immers een veiligheidscultuur bewerkstelligen bij zijn collega's. De bedrijfsdirectie moet hem steunen en zelf het voorbeeld geven. Alle middelen zijn goed om te sensibiliseren: affiches aan de muur, zelfs in de toiletten (echt waar!), mails ter herinnering aan de veiligheid, een Cyber Security Beleid opnemen in het arbeidsreglement, de infrastructuren regelmatig testen, jaarlijks conferenties en opleidingen organiseren om de praktijken te herhalen. We moeten de werknemer doen begrijpen dat hij verantwoordelijk is voor zijn handelingen die een impact kunnen hebben op de bedrijfsveiligheid. We moeten ook doen begrijpen dat veiligheid niet zomaar een IT-kwestie is maar ook een menselijk aspect heeft (Social engineering[102]).

Voor de **kleine structuren zoals kmo's of soho's** die niet in staat zijn een voltijds Cybersecurityexpert aan te werven, bestaan er twee oplossingen:

- Een informaticus aanwerven met algemene vaardigheden die (na een korte opleiding) tijd kan besteden aan de veiligheid.
- Een beroep doen op consultancy bedrijven die gespecialiseerd zijn in beveiliging (we merken op dat dit soort bedrijven in volle opmars zijn door de grote behoefte op de markt).

101. http://www.childfocus.be/nl/preventie/clicksafe-veilig-internetten
102. Social engineering: zie woordenlijst

4. Financiële bijstand en administratieve ressources om de ondernemingen te adviseren

Hoe kunnen we de goede praktijken van informatiebeheer doorvoeren binnen een kmo of microbedrijf? In Brussel is er geen enkele financiële bijstand voorzien om de overgang van de bedrijven naar meer bewustzijn voor veiligheid te faciliteren. Het Waalse Gewest biedt financiële steun en fiscale aftrek voor kmo's die in digitale oplossingen investeren. Maar slechts weinigen zijn hiervan op de hoogte. We moeten die hulp dus meer onder de aandacht brengen en de context en details ervan communiceren. Er zijn twee categorieën "Cybersecurity cheques" voor de ondernemingen: de Audit cheque (bepaling van een *privacy by design* veiligheidsbeleid) en de cheque 'labellisation coaching' (erkenning coaching) (evaluatie om een kwaliteitslabel te verkrijgen)[103]. Deze initiatieven werden opgericht omdat men vaststelde dat de kmo's zich wel bewust zijn van de problematiek rond Cybersecurity (zie hoofdstuk over kmo's) maar niet over de middelen beschikken om een Cybersecuritystrategie in te voeren. Dit zijn heel interessante steunmaatregelen en het Brussels Hoofdstedelijk Gewest zou ook moeten nadenken over bijstand voor ondernemingen.

Laten we ook de instellingen niet vergeten die begeleiding en advies bieden aan bedrijven die net starten of hun onderneming willen verbeteren. In ons verslag hebben we het platform 1819[104] en de bedrijfsincubator Impulse.Brussels[105] besproken.

5. De overheid moet een rol spelen

Cybersecurity wordt hoofdzakelijk geassocieerd aan het federaal niveau zelfs als de activiteiten steeds meer op regionaal niveau worden gevoerd. Het Brussels Hoofdstedelijk Gewest en haar overheidsdiensten moeten een rol spelen: ze moeten niet enkel begeleiden en adviseren maar ook sensibiliseren. De media, die ons het nieuws over cybercriminaliteit brengen, laten ons geloven dat deze bedreigingen vooral op overheidsinstellingen zijn gericht. Maar daar stopt het niet. Deze problematiek treft iedereen! De overheid moet dus transparant zijn en het voorbeeld geven; aantonen dat iedereen een mogelijk doelwit is. Het is immers niet omdat wij denken dat we geen gevoelige gegevens behandelen dat hackers geen interesse in ons hebben. De eerste stap in de sensibilisering is **de informatie centraliseren** op referentiewebsites voor alle doelgroepen en deze ook promoten zodat de betreffende doelwitten de reflex krijgen om deze sites regelmatig te raadplegen.

6. De kloof tussen de beschikbare profielen op de arbeidsmarkt en het aantal vacatures wegwerken

We moeten rekening houden met meerdere criteria. Ten eerste zijn er sinds enkele maanden, vanwege de Europese maatregelen, nieuwe opleidingen beschikbaar voor elk publiek. Ondanks alles mankeren deze opleidingen in Cybersecurity zichtbaarheid. Vervolgens is het zo dat er in België geen duidelijke referentielijsten bestaan van de beroepsprofielen en dat ze vaak met een slecht imago kampen. Ten slotte moet de manier van aanwerven veranderen. Professionele ervaring mag niet langer het belangrijkste criterium zijn bij de aanwerving. Zoals we in het hoofdstuk over de beroepen zagen, heeft een studie vastgesteld dat atypische profielen ook vaak goede profielen zijn. Zo zijn ook de *soft skills* heel belangrijk in de Cybersecurity profielen. In een eerste fase moeten de opleidings- en tewerkstellingsactoren duidelijke referentielijsten opstellen om zo de behoeften van de bedrijven en de te verwerven vaardigheden beter op elkaar te kunnen afstemmen. Vervolgens moet de academische wereld opleidingen ontwikkelen en voorstellen voor alle

103. https://www.e-net-b.be/page/wallonie-nouveaux-subsides-2017-pour-les-entreprises-aides-au-numerique.html
104. http://www.1819.be/fnl ⇒ http://www.1819.be/nl
105. http://www.abe-bao.be/nl

soorten profielen (lange opleidingen, korte en kwalificerende opleidingen, etc.). Door de problematiek te analyseren hebben we ontdekt dat de opleidingen veiligheidsexperts moeten vormen die een roeping hebben en niet enkel technische vaardigheden. De opleidingen moeten dit opnemen in hun lesaanbod zodat de lessen aangepast zijn aan de realiteit op het terrein.

7. Veille, sensibilisation et formation IT : le Pôle Formation Emploi ICT aura un rôle à jouer

De Opleidings- en Tewerkstellingspool voor ICT gaat van start tegen eind 2018. Hij zal een rol spelen in de promotie, communicatie en opleidingen van Cybersecurity in:

- Het aanbod van opleidingen in Cybersecurity van korte duur voor werkzoekenden, werknemers, leerkrachten en trainers en voor studenten. Deze opleidingen worden ingevuld met technische lessen en informaticalessen maar ook het juridische aspect komt aan bod (voorbeelden: opleiding GDPR, opleiding soft skills …).
- Het aanbod van lange kwalificerende opleidingen en/of specialisatie voor werkzoekenden.
- Het overbrengen van een boodschap via deelname aan en organisatie van evenementen (conferenties, hackathons[106], samen met andere instellingen deelnemen aan diverse gevarieerde evenementen).
- De promotie van de beroepen en de sensibilisering zijn belangrijke assen voor de pool. Zoals we reeds hebben uiteengezet in het verslag is het belangrijk om de allerjongsten te sensibiliseren via de leerkrachten en ouders. De pool kan de volwassenen pedagogische hulpmiddelen geven waarmee ze de kinderen kunnen sensibiliseren.

106. Hackhatons: zie woordenlijst

Dankbetuigingen

Om dit rapport op te stellen hebben we een beroep gedaan op vakexperten die hun kennis en knowhow inzake Cybersecurity met ons wilden delen. We bedanken hen van harte voor hun tijd en aandacht.

Jean-Marc André - UNIWAN

Olivier Bogaert - FCCU

Andries Bomans – CCB

Ferdinand Casier - AGORIA

Thierry Cools - Bruxelles formation

Marc Daem – CIBG

Vincent Defrenne - NVISO

Florianne de Kherchove – AGORIA

Tanguy De Lestré – Kabinet van Staatssecretaris in het Brussels Hoofdstedelijk Gewest Bianca Debaets

Benoit Fosty – CIBG

Jeroen Franssen – AGORIA

François Goffinet – Sinibaldi

Nicolas Harmel – Kabinet van minister Didier Gosuin, minister van Economie en Tewerkstelling in Brussel

Jean-Jacques Quisquater – UCL

Grégorio Matias – MCG

Philip Richardson – Bruxelles formation

Benoit Rousseaux – Digital Security

Bruno Schröder - Microsoft, MIC

Valery Vander Geeten – CCB

Pascal Van de Walle - CIBG

Nicolas Vautrin – INNOVIRIS

Woordenlijst

Bitcoin : cryptografisch geld en een peer-to-peer betaalsysteem. Bron – Wikipedia.

Compliance : conformiteit.

Cyber-résilience : capaciteit om zich voor te bereiden op, en aan te passen aan constant evoluerende situaties, en ook snel opnieuw kunnen handelen na aanvallen, ongevallen, natuurrampen of incidenten, binnen het kader van het gebruik van informatie- en communicatiemiddelen. Bron definitie: http://www.ab-consulting.fr/blog/non-classe/cyber-securite-vs-cyber-resilience

Encryptie : procedé uit de cryptografie dat bestaat uit het onleesbaar maken van gegevens (versleutelen) voor personen die geen sleutel hebben.

Forensische wetenschappen : forensische analyse in de informatica betekent de analyse van een informatiesysteem na een incident. Bron: Wikipedia.

Hackathon : een evenement van enkele dagen waar vrijwillige ontwikkelaars samenkomen om te programmeren. Het is een creatief proces dat vaak wordt gebruikt op het gebied van digitale innovatie. Bron: Wikipedia.

Hacking : of softwarepiraterij. Allerlei technieken waarmee men gebreken en kwetsbaarheden van een materieel of menselijk systeem uitbuit.

Malware : kwaadaardige software (programma's) die een informatiesysteem aantast.

MOOC : Massive Open Online Course. De MOOC is een massale open online cursus te vergelijken met een open opleiding op afstand.

NotPetya: ransomware van hetzelfde type als WannaCry.

Phishing : een fraudetechniek die bestaat uit het verwerven van persoonsgegevens om er identiteitsfraude mee te plegen. Bron: Wikipedia.

Pop-Up : een venster dat ongevraagd bovenop het bestaande venster verschijnt terwijl men op het internet surft. Bron: Wikipedia.

Privacy by design : het principe om de gegevens te beveiligen zodra het informatiesysteem of -netwerk is ontworpen en werkt, maar ook verantwoorde praktijken uitwerken.

Ransomware : kwaadaardige software die persoonsgegevens gijzelt. Het slachtoffer moet losgeld betalen om zijn gegevens te recupereren.

Social engineering : of social hacking. Deze techniek verwijst naar psychologische manipulatie om te kunnen oplichten. De oplichters maken misbruik van psychologische en sociale zwakte, en in ruimere zin van organisatorische zwaktes om iets van een bepaald persoon te verkrijgen (een bezitting, een dienst, een bankoverschrijving, fysieke of logische toegang, verspreiding van vertrouwelijke informatie, etc.). Bron: Wikipedia.

Wannacry: ransomware die een veiligheidsgebrek van Microsoft Windows uitbuit. Deze ransomware heeft zich ongetwijfeld verspreid via een massale mailingcampagne. Eens het virus is geïnstalleerd en de bestanden versleuteld, vraagt het virus losgeld in bitcoins.

White paper: of witboek. Verzameling van objectieve informatie die bestemd is voor een bepaald publiek om over een bepaald onderwerp te kunnen beslissen. Bron: Wikipedia.

Geciteerde organisaties

CCB : Centre for Cybersecurity Belgium http://www.ccb.belgium.be/nl

CEIS : Compagnie Européenne d'Intelligence Stratégique https://ceis.eu/fr/accueil/

CIRB : Centrum voor Informatica voor het Brusselse Gewest http://cibg.brussels/nl

BELNET : Belgisch nationaal onderzoeksnetwerk dat internettoegang aan zeer hoge bandbreedte en internetdiensten levert aan universiteiten, hogescholen onderzoekscentra en overheidsdiensten. https://www.belnet.be/nl

FCCU: Federal computer crime unit. https://www.police.be/5998/nl/over-ons/centrale-directies/federal-computer-crime-unit

ENISA: European Union Agency for Network and Information Security https://www.enisa.europa.eu/media/enisa-en-francais/

OCDE : Organisatie voor Economische Samenwerking en Ontwikkeling. http://www.oecd.org/fr/

PFE : Opleidings- en tewerkstellingspool voor ICT

REDACTEUR
Christina Galouzis

POST EDITOR
Luc Huygh

VERANTWOORDELIJKE UITGEVER
Jean-Pierre Rucci

GRAFISCH ONTWERP
www.sergeantpaper.be

DRUK
Boarding Concept
4 Place André Duchêne
1160 Auderghem
www.boardingconcept.be

CONTACT
vzw Evoliris
Paalstraat 14 A I 1080 Brussel I 02/475 20 00
info@evoliris.be I www.evoliris.be

Evoliris

De vzw EVOLIRIS is het Beroepenreferentiecentrum voor de ICT –sector (Informatie- en communicatietechnologieën) van het Brussels Hoofdstedelijk Gewest. Vanaf zijn oprichting in 2006 zet het centrum zich in voor de sensibilisering, informatie en opleidingen van de ICT-beroepen. EVOLIRIS is voornamelijk actief bij drie doelgroepen: **leerlingen en leerkrachten** in het kader van sensibiliseringscampagnes voor de beroepen, **werkzoekenden** dankzij onze opleidingen en begeleiding bij het zoeken naar werk. En ten slotte **voor werknemers**, in het bijzonder de werknemers die dankzij onze opleidingen verder kunnen evolueren in hun vakgebied.

Voor meer info : **www.evoliris.be**

Contact :

Paalstraat 14 – Gebouw A I 1080 Brussel 02 475 20 00 I info@evoliris.be