LES CAHIERS D'EVOLIRIS #2

APRÈS LA SENSIBILISATION

État des lieux sur la Cybersécurité à Bruxelles

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 et CEO chez CISCO

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

Table des matières

Préface

L'informatique est un terrain vivant en pleine évolution. Evoliris, depuis sa création, tente à son niveau de suivre les évolutions technologiques afin d'en comprendre les conséquences et les implications sur le marché de l'emploi et de la formation.

Chaque année, la courbe des tendances de Gartner présente l'évolution des tendances technologiques. En 2017*, cette analyse montre que le Big Data, l'Intelligence Artificielle, l'Internet of Things, la réalité augmentée et les technologies de la Cybersécurité sont en plein boom.

Au regard de l'évolution de la criminalité virtuelle, la Cybersécurité est une tendance au centre des préoccupations des responsables, tant informatiques que politiques et sociétaux. En Belgique, en Europe et à travers le monde, de nombreuses initiatives insistent sur l'importance de s'adapter et de sensibiliser les acteurs économiques et sociaux aux menaces qui se développent sur le net.

Et pour cause : le mois de mai 2017 a été le théâtre d'attaques de grandes envergures (Wannacry, NotPetya entre autres). Il n'y a rien de nouveau, sauf que ce qui change cette année, c'est le rôle qu'ont pris les médias dans la diffusion de l'information. Tout à coup, le citoyen - c'est-à-dire vous et nous - s'est rendus compte que son univers virtuel n'était pas infaillible et que les méthodes pour nous soustraire des données privées et sensibles sont très abouties.

C'est le rôle d'Evoliris, et demain celui du Pôle Emploi Formation ICT, de concrétiser la volonté de développer la veille sectorielle, entre autres de la Cybersécurité, en vue d'assurer l'adaptation de formations proposées par le Pôle aux évolutions des métiers.

L'objectif du présent document consiste à mesurer à travers plusieurs axes de réflexion l'impact et la place de la Cybersécurité sur la Région de Bruxelles-Capitale tant en termes d'activités économiques, d'orientation politique, d'emploi ou de formation. L'action politique (européenne, fédérale ou régionale), la gestion de la sécurité informatique en entreprise, le secteur académique et l'analyse du recrutement jouent un rôle important dans l'évolution de la Cybersécurité à Bruxelles. Des experts belges, par leurs témoignages, nous ont permis de rédiger ce document en phase avec la réalité de terrain.

Sensibilisation, mixité, réglementations fédérales ou européennes, profils-métiers et paysage de formation à Bruxelles sont les sujets développés dans ce rapport qui constitue notre deuxième « **Cahier d'Evoliris** ». Bonne lecture !

Jean-Pierre Rucci
Directeur d'Evoliris

Pierre Merveille
Président d'Evoliris & Secrétaire responsable des secteurs Finances - Services - Industrie à la SETCA

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

1 Introduction

Chaque jour, plus de 5 millions de données sont volées ou perdues à travers le monde, cela représente plus de 200 000 données par heure[1].
En Belgique, déjà en 2009, on comptabilisait 68 millions d'euros de dommages liés à des fraudes selon la Federal Computer Crime Unit (FCCU)[2].

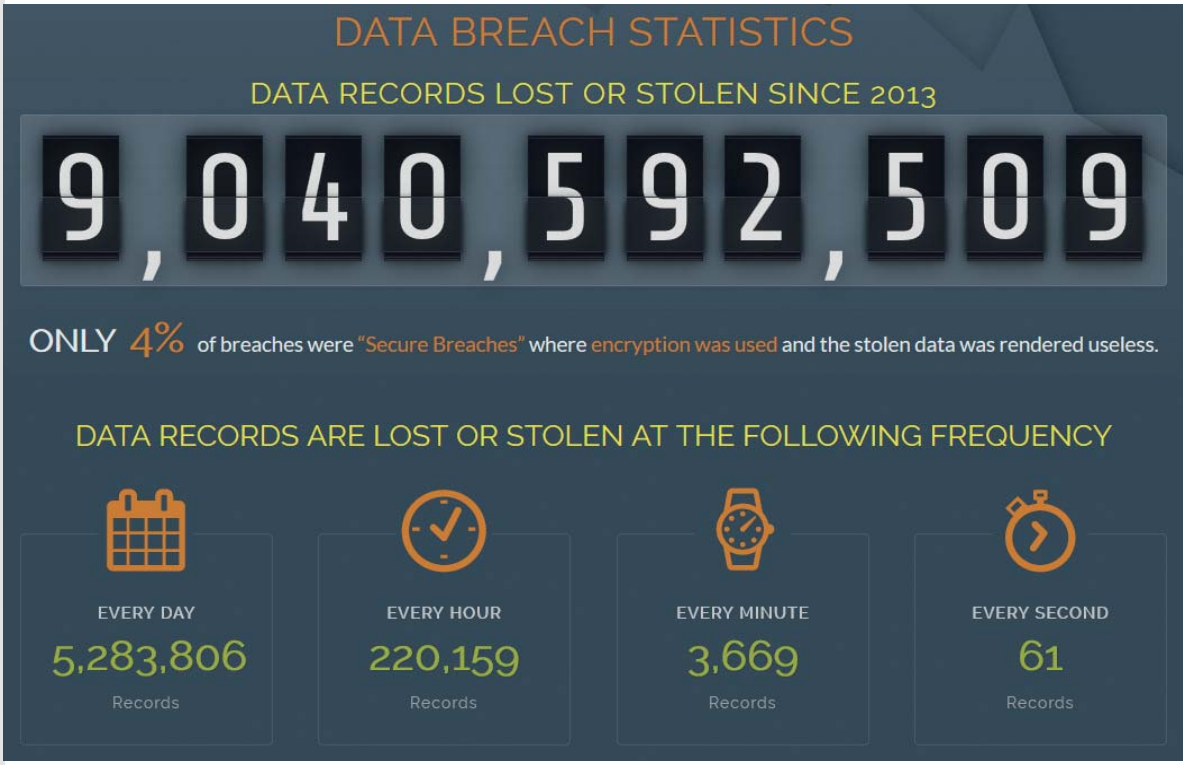


Figure 1 - Breach Level Index. Source: http://breachlevelindex.com

Ces chiffres nous montrent clairement que la Cybersécurité, la sécurité des données, est un véritable enjeu. C'est un enjeu du point de vue **technologique** avec le développement d'outils performants pour détecter les attaques. C'est aussi un enjeu **politique**. La régularité des attaques de plus en plus nombreuses incite les pays à travers le monde à mettre en place des stratégies de Cybersécurité au niveau national. C'est enfin un enjeu **économique** et **sociétal**, car les métiers liés de près ou de loin à la sécurité sont en émergence. Aujourd'hui, la digitalisation est une réalité. Elle l'est et ça, les hackeurs l'ont bien compris.

Aujourd'hui, il n'est pas rare de découvrir un article dans nos quotidiens concernant une brèche de sécurité importante ou un vol de données. Wannacry[3], NotPetya[4], ces noms ne vous sont sans doute pas inconnus.

Plus localement, la Cybersécurité touche l'économie entrepreneuriale bruxelloise, les métiers et le monde de l'enseignement. C'est une thématique qui reste la préoccupation avant tout du point de vue du fédéral, mais aussi du secteur public, des entreprises et des citoyens.

1. http://breachlevelindex.com
2. « La Cybersécurité est un enjeu pour tous » gras Gaëtan Dans LaLibre.be [en ligne] http://www.lalibre.be/economie/digital/la-cybersecurite-est-un-enjeu-pour-tous-51b732d1e4b0de6db9756ab2
3. Wannacry : voir glossaire.
4. NotPetya : voir glossaire.

1.1 Pourquoi étudier la Cybersécurité à Bruxelles ?

La veille sectorielle fait partie des missions d'Evoliris. Cette veille s'effectue dans le but de proposer des formations, des recommandations ou des conseils adaptés aux exigences actuelles.

La finalité, en particulier, de ce rapport consiste à dépeindre la situation de la Cybersécurité en région bruxelloise. En effet, à Bruxelles, l'impact des menaces informatiques est intéressant à analyser en termes de formations, de métiers et de gestion de la sécurité en entreprise. Par conséquent, cela nous permet de voir comment Bruxelles à travers sa politique, ses mesures au niveau du secteur IT et de la formation, réagit pour répondre à cette nouvelle forme de menace et comment la Région de Bruxelles-Capitale devra évoluer dans les années à venir. D'ailleurs, en 2013 déjà, le Premier ministre Elio Di Rupo déclarait concernant la création du Centre pour la Cybersécurité Belgique[5]: « *la sécurité c'est aussi la protection de la vie privée, de nos intérêts économiques et de l'appareil de l'État*[6]». Les conclusions de ce rapport nous permettront de comprendre la situation de Bruxelles face à cette problématique et de proposer des actions à mener à l'avenir.

1.2 La méthodologie

Afin de délimiter les axes principaux de ce sujet, Evoliris a débuté sa réflexion par une table ronde réunissant des experts en Cybersécurité. Cette table ronde a été organisée le 31 mai 2017 avec la participation de deux membres d'Evoliris et de 5 experts :

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

Elle nous a permis de dégager une série de questions et de constats que nous développerons dans ce rapport. Suite à cela et afin d'approfondir ces questions, nous avons poursuivi notre enquête avec des entretiens individuels auprès d'autres experts (la liste des experts consultés se trouve en fin de rapport dans le chapitre « Remerciements »). Sur la base de ces entretiens qualitatifs, nous avons élaboré ce rapport de synthèse. Par ailleurs, des conclusions et recommandations sont proposées en fin de rapport.

Dans ce document, nous présentons, à travers plusieurs axes de réflexion issus de la réalité de terrain, un état des lieux qui part d'une série de questions :

- Quelle est la place de la problématique de la Cybersécurité en Région de Bruxelles-Capitale ?
- Quel est le niveau de maturité de Bruxelles ?
- Quel est l'impact de la Cybersécurité dans l'évolution des métiers ?
- Quelles compétences recherche-t-on dans les profils liés à la Cybersécurité ?
- Quelles mesures sont prises par et pour les entreprises ?
- Quels moyens consacre-t-on à la sensibilisation des entreprises et des citoyens ?
- Comment le secteur de la formation répond-il au besoin de recrutement dans la sécurité informatique ?

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

1.3 La Cybersécurité : délimitation du sujet

La Cybersécurité est un terme générique qui englobe la problématique de différents types d'attaques informatiques, tout en tenant compte de la digitalisation toujours plus présente et des menaces qui augmentent en proportion.

Aujourd'hui, on estime que la Belgique représente 16% des attaques de malwares[7] en Europe. Ce n'est ni plus ni moins que le deuxième pays le plus attaqué après l'Allemagne selon le graphique en figure 2. Les secteurs les plus touchés par ces attaques sont :

- Le secteur financier,
- Le secteur marchand,
- Les administrations publiques[8].

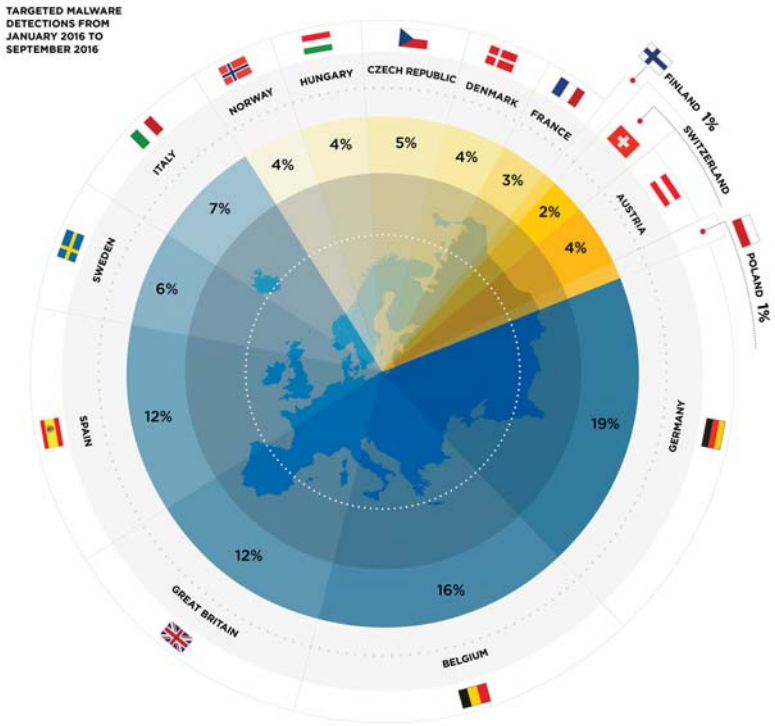
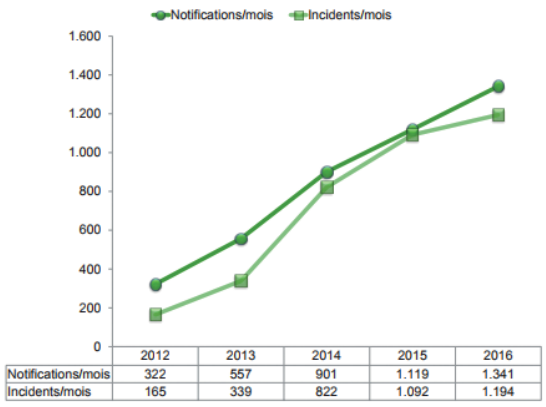


Figure 2 - Menace Malware détections de janvier 2016 à septembre 2016. Source : https://www2.fireeye.com/rs/848-DID-242/images/Infographic_GDPR.pdf



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

On note également que le nombre d'incidents recensés par BELNET est en augmentation constante depuis 2012[9].

Figure 3 - Nombre de notifications et d'incidents réels (par mois). Source BELNET

C'est pourtant grâce à des attaques d'envergure comme Wannacry ou NotPetya (entre autres) que l'on a pris conscience du problème via la presse. Des actions de sensibilisation se mettent en place afin de réduire l'impact de ces menaces. Mais est-ce suffisant ?

7. Malware : voir glossaire
8. https://www2.fireeye.com/rs/848-DID-242/images/Infographic_GDPR.pdf
9. http://economie.fgov.be/fr/binaries/Barometre_de_la_societe_de_l_information_2017_tcm326-284038.pdf

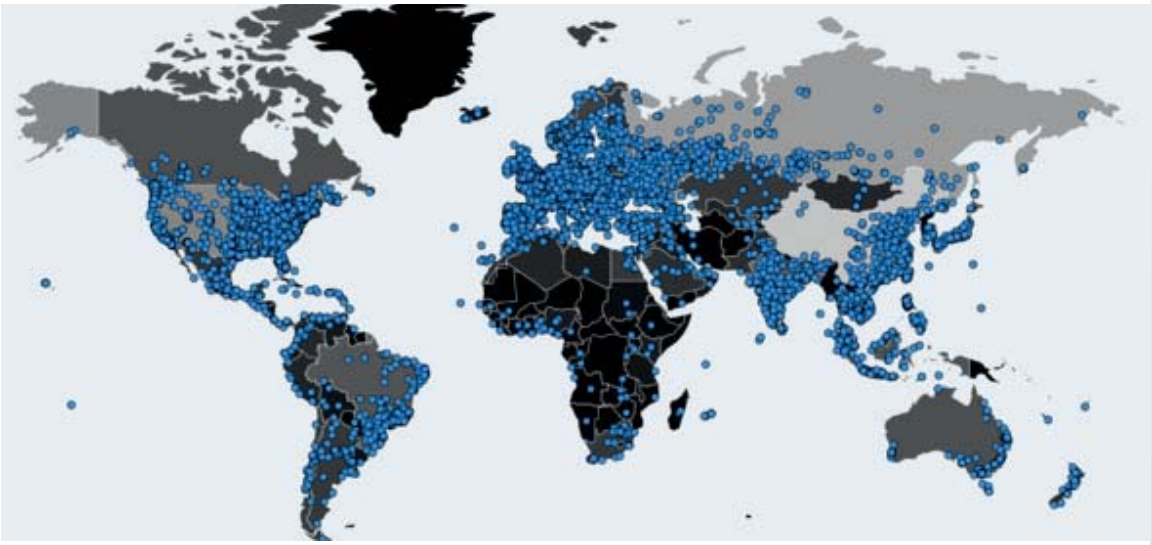


Figure 4 - Source Image : MalwareTech.com

En mai 2017, l'attaque du Ransomware Wannacry d'envergure mondiale a fait plus de 300.000 victimes[10].

Wannacry est un ransomware[11] (rançongiciel) qui exploite une faille de Microsoft Windows. Ce ransomware s'est sans doute diffusé par une campagne de mailing massif. Une fois le virus installé et les fichiers encryptés, le virus demande une rançon en bitcoin.

Wannacry a perturbé un grand nombre d'établissements critiques ou importants comme des hôpitaux britanniques ou le Ministère de l'Intérieur Russe. On estime que 150 pays ont été touchés par ce malware. Selon Europol, 200 000 ordinateurs auraient été atteints par le virus[12].

En Belgique, l'impact est resté limité. Quelques PME ont envoyé un signalement au CCB (Centre pour la Cybersecurity Belgique). La société Q-Park a notamment été touchée[13].

1.4 La cybercriminalité, une histoire qui remonte aux années 80

Alors, voilà tout un cahier où on vous parle de cybercriminalité ou de Cybercrime. Mais c'est quoi, en définitive ? Si on en croit Wikipedia, le Cybercrime, *c'est une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel, le « cyberespace ». Depuis quelques années, la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement du Cybercrime*[14]. En réalité, c'est plus compliqué.

À l'origine, les ordinateurs, les réseaux informatiques et Internet ont été créés dans le but d'échanger une série d'informations dans un espace virtuel qui dépasse les frontières physiques. Les données (personnelles, bancaires, professionnelles, etc.,) deviennent un enjeu commercial pour un grand nombre d'individus malhonnêtes. Les profits liés au vol d'identité, d'informations bancaires, et autres secrets professionnels ont créé une industrie plus que lucrative.

10 « Ransomware : le nettoyage se poursuit après le chaos Wannacry », ZDNet France, 2017 [en ligne] http://www.zdnet.fr/actualites/ransomware-le-nettoyage-se-poursuit-apres-le-chaos-wannacry-39852650.htm
11. Ransomware : voir glossaire.
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://fr.wikipedia.org/wiki/Cybercrime

La cybercriminalité apparaît dans les années 80 sans que pour autant, on vous vole quoi que ce soit en ligne. Vous vous souvenez sans doute du célèbre Prince nigérien qui vous demande votre aide et votre argent pour débloquer une somme d'argent colossale bloquée en Angleterre. Pour vous remercier de votre effort, ce bienfaiteur vous promet 10% de cette belle somme.

Ensuite, il y a eu les arnaques avec les navigateurs ayant des failles de sécurité. Vous visitiez un site (souvent peu recommandable, on ne va pas se le cacher) qui installait quelque chose dans votre navigateur, ce qui faisait apparaître une multitude de « pop ups[15]».

Mais c'est dans les années 90 que les choses sont devenues sérieuses, notamment avec l'avènement du World Wide Web en 1994. C'est à ce moment-là que les criminels du web ont découvert la fusion de sites web (des gestionnaires de contenus), qui incorporaient des bases de données personnelles (des clients, des membres ou des visiteurs par exemple). Il était très facile d'accéder à ces bases de données à partir de l'interface web de l'organisation. C'était une véritable caverne d'Ali Baba pour les cybercriminels.

Dans ce chapitre, nous n'avons pas encore parlé des virus. Pourtant, c'est le premier mot qui nous vient à l'esprit quand on parle de Cybercrime. Il fut un temps où on s'amusait à propager des virus simplement pour ennuyer son monde. Le virus « Elk Cloner[16]» est l'un des premiers, conçu pour l'Apple II (1982). Il sera suivi par tout une série d'autres virus tous plus malveillants les uns que les autres.

Au fil des années, des petits plaisantins se sont succédé pour pirater des programmes nucléaires coréens, la NASA et d'autres institutions internationales comme la CIA. Viennent ensuite les macrovirus écrits dans des langages informatiques associés aux applications et qui se lancent donc, dès que vous ouvrez vos applications. C'est une nouveauté, car avant, un virus était un programme séparé.

L'histoire de la cybercriminalité est directement liée à l'évolution des technologies informatiques. Elle ne cesse de se développer et de se complexifier. Ce petit chapitre a été une mise en bouche. Vous voulez en savoir plus ? Lisez cet article[17] vantant les mérites de la connexion VPN, ainsi que celui-ci[18], relatant l'histoire du Cybercrime par Symantec, un des grands joueurs en matière de protection.

La cybercriminalité a un passé prolifique et un bel avenir devant elle. Voyons à présent l'impact de la cybercriminalité et de la Cybersécurité à Bruxelles.

15. Pop-Up : voir glossaire.
16. https://en.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

Une économie bruxelloise de la Cybersécurité

2

- 5 points pour évaluer la maturité de la Région -

Lors des entretiens avec les experts, la possibilité que la Région de Bruxelles-Capitale puisse être une ville européenne de la Cybersécurité a été évoquée. Dans ce rapport, c'est à travers 5 points essentiels de la vie politique et économique bruxelloise que nous évaluons cette problématique.

2.1 Ce que veulent les politiques

Il est intéressant de s'interroger sur les actions parlementaires bruxelloises au niveau de la sécurité informatique.

Selon M. Nicolas Harmel, attaché au cabinet de M. Didier Gosuin, ministre de l'Économie, de l'Emploi, de la Formation, de la Santé, du Budget et de la Fonction publique, « *dans le contexte de la régionalisation de l'état, la question de la Cybersécurité est encore fortement morcelée. La plupart des actions sont mises en œuvre au travers du CIRB (Centre Informatique pour la Région Bruxelloise)* ».

Néanmoins, « *étant donné que les institutions publiques sont de plus en plus souvent les cibles des attaques organisées, des questions parlementaires sont de plus en plus fréquentes sur le sujet* » annonce M. De Lestré, conseillé en Informatique et Transition Numérique au Cabinet de la Secrétaire d'État Bianca Debaets chargée notamment de l'Informatique régionale et communale et de la transition numérique.

Ainsi, la préoccupation principale des parlementaires bruxellois est de s'assurer de la sécurité des infrastructures qui hébergent les systèmes et bases de données publiques. Les actions de sensibilisations aux citoyens ne sont donc pas leur rôle malgré des initiatives comme le plan NextTech[19]. À travers ce plan régional, on retrouve cette volonté de veille et de sensibilisation à la problématique de la Cybersécurité. La mesure 16 qui concerne la création du Pôle Formation Emploi ICT, concrétisera la volonté de développer et de rendre accessible les formations et les aides à l'emploi dans le secteur de l'IT à Bruxelles. La veille sectorielle sera développée dans le but d'assurer l'adaptation des formations proposées par le Pôle aux évolutions des métiers. Or, les métiers de la Cybersécurité sont en pleine évolution et cela ne risque pas de s'arrêter dans les années à venir. L'analyse des données sur le recrutement met en évidence un manque croisant de profil qualifié. D'ici 2020, la Belgique sera en manque de 2000 experts en Cybersécurité[20]. C'est notamment avec la formation et la promotion du secteur que le Pôle pourra répondre aux besoins de maturité de Bruxelles.

Enfin, dans le paysage institutionnel, il faut distinguer les compétences régionales et fédérales. Traditionnellement, la gestion de la Cybersécurité et de la Cybercriminalité est du ressort des instances politiques fédérales qui se chargent de mettre en place des mesures pour renforcer la sécurité. « *Il est clair cependant que la Cybersécurité est une affaire qui tient du fédéral plutôt que du régional. Néanmoins, le régional doit coopérer dans cette mission de sécurité* », déclare M. Ferdinand Casier, Business Group Leader Digital Industries chez Agoria.

19. https://nexttech.brussels/
20. https://www.digitalwallonia.be/centre-cybersecurite-thales/

2.2 Création du CCB et centralisation des instances fédérales

L'action fédérale s'est notamment organisée à travers la création du CCB (Centre pour la cybersécurité Belgique[21]) qui a permis de centraliser les actions liées à la Cybersécurité. Avec l'appui de son service CERT.be, le CCB gère les situations de crise liées aux cyberattaques et donne des recommandations en matière de sécurité des systèmes et réseaux d'information à l'égard du secteur public et des opérations de service essentiel. Ces recommandations sont conçues afin de faciliter le travail en amont et permettre aux institutions tant publiques que privées de se prémunir des cyberattaques et de savoir qui contacter en cas d'urgence. C'est aussi le rôle du CCB de sensibiliser les institutions sur les pratiques de sécurité et sur les aides et outils belges à disposition.

« *Il faut centraliser les informations ! L'objectif est d'avoir une plateforme de référence pour les entreprises et une plateforme de référence pour le grand public* » dit M. Olivier Bogaert, de la FCCU (Federal Computer Crime Unit). Cette déclaration de M. Bogaert pose le doigt sur l'objectif principal du CCB : réunir les acteurs fédéraux de la Cybersécurité pour proposer une plateforme unique d'information qui fera office de référence.

Focus sur le CCB

CENTRE FOR CYBER SECURITY BELGIUM

Fondé par l'arrêté royal du 10 octobre 2014, le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale compétente en matière de sécurité des systèmes et réseaux d'information en Belgique. Il a notamment pour mission de coordonner et de centraliser les projets et les politiques en matière de Cybersecurité. Depuis 2017, le service CERT.be («*Computer Emergency Response Team*», c'est-à-dire l'équipe d'intervention d'urgence en sécurité informatique) géré par BELNET a été intégré au sein du CCB. Le CCB accorde une grande importance à la sensibilisation du public. C'est pourquoi il organise chaque année une campagne nationale de sensibilisation. En 2017, le thème de la campagne fut la lutte contre le « Phishing ».

Le site web du CCB et du CERT.be propose de brochures et de renseignements utiles. Ceux-ci s'adressent à tous les publics : citoyens, entreprises, écoles, autorités publiques et secteurs vitaux (le secteur de l'énergie, de la mobilité, des soins de santé, le secteur financier, etc).

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

2.3 S'inspirer des initiatives européennes

Au niveau européen, la Cybersécurité est aussi un sujet de débat. En 2016, la Commission européenne a lancé un projet de partenariat public-privé en investissant 450 millions pour développer la recherche et le développement en lien avec la Cybersécurité[22]. Le secteur privé devrait injecter 1,35 milliard dans les projets d'ici 2020. Ce financement est en projet depuis 2013 avec la création d'une note sur la « Stratégie de Cybersécurité de l'Union Européenne[23]» .

Cette note présente cinq objectifs prioritaires :
- « *parvenir à la cyber-résilience[24];*
- *réduire considérablement la cybercriminalité;*

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 : voir glossaire

- *élaborer une politique de cyberdéfense ainsi que des capacités relevant de la politique de sécurité et de défense commune de l'UE (PSDC);*
- *développer les ressources industrielles et technologiques nécessaires à la Cybersécurité;*
- *instaurer pour l'UE une politique internationale cohérente en matière de cyberespace*[25] ».

En conclusion, les actions européennes se concrétisent en plusieurs axes :

- **Conseils et sensibilisation :** avec la création d'action comme le European Cyber Security month[26] (ou CyberSecMonth). Chaque année, en octobre, et ce depuis 5 ans déjà, la Commission Européenne sensibilise à la Cybersécurité. À travers toute l'Europe, des activités et événements de sensibilisation sont organisés,
- **Mise en place de mesures et réglementations pour structurer la Cybersécurité**[27]**:** la Commission Européenne a mis en place l'application de mesures structurantes pour les entreprises comme la réglementation GDPR (General Data Protection Regulation) ou la directive NIS (Network and Information Security) que nous détaillerons dans un prochain chapitre,
- **Centralisation des moyens et actions européennes :** en septembre 2017, la Commission européenne a présenté une nouvelle agence de Cybersécurité . Cette agence, fondée sur les actions de l'Agence de Sécurité des Réseaux et de l'Information (Enisa) pourra accorder des certificats garantissant la fiabilité des services et produits numériques concernés.

Au final, ces actions de la Commission Européenne se concrétisent par la volonté de mettre en place un plan stratégique au niveau européen dans le but d'apporter une base européenne aux états-membres.

2.4 Le Pôle Formation Emploi ICT : le rôle économique des formations

Aujourd'hui, il y a un écart important entre la disponibilité des profils qualifiés sur le marché belge de l'emploi et les offres de recrutement en pleine explosion. Ce problème est en partie impacté par le manque de formations liées à la Cybersécurité en Belgique. Les formations existantes ne fournissent pas assez d'experts de la Cybersécurité pour répondre aux demandes du secteur. Ce problème est connu, c'est pourquoi depuis quelques mois, plusieurs offres de formations ont vu le jour. Des formations universitaires, des bacheliers, des cours intégrés dans des cursus remodelés ou des formations qualifiantes, ce sont autant de nouvelles possibilités qui permettront demain d'accéder à un métier en pleine émergence. Il faut néanmoins que ces formations puissent offrir des compétences en accord avec les besoins des entreprises. Il est important d'ouvrir un dialogue entre les institutions académiques et les entreprises. Ce sera notamment le rôle du PFE : le Pôle Formation Emploi ICT de Bruxelles. Le Pôle Formation Emploi ICT devrait voir le jour d'ici la fin de l'année 2018, le fonctionnement sera assuré par une contribution publique et privée. Le Pôle Formation ICT émane de la volonté politique régionale de créer une institution qui centralise les acteurs de la formation et de l'emploi dans le secteur de l'IT. Il aura donc pour rôle de « *renforcer l'organisation, le développement et la promotion de la formation et de l'emploi dans le secteur visé, ainsi que la sensibilisation aux métiers ICT, en soutien au développement économique et social du territoire bruxellois*[28]» .

25. http://www.consilium.europa.eu/fr/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
28. https://nexttech.brussels/wp-content/uploads/2017/01/PlanNextTech-2017-2020-fr.pdf

2.5 Bruxelles n'est pas encore prête pour être la capitale de la Cybersécurité

Tout au long des différentes entrevues que nous avons eues en préparation à ce cahier que vous tenez entre vos mains, il s'est dépeint une image exceptionnelle de Bruxelles. En effet, bon nombre de nos interlocuteurs mettent l'accent sur la valeur symbolique de Bruxelles comme capitale de l'Europe. Et en effet, Bruxelles peut être petite en taille, mais cette ville de plus d'un million d'habitants héberge tout de même plusieurs hauts lieux de L'Union Européenne (la Commission, le Parlement), l'OTAN, Eurocontrol. Pour cette raison, s'y sont installées également plusieurs antennes d'organisations mondiales (le Conseil de l'Europe, l'Organisation des Nations Unies, l'UNESCO, la Banque Mondiale, etc.). Tout ce beau monde attire bon nombre de sociétés qui dépendent d'une façon ou d'une autre d'une de ces organisations internationales. Mais le côté obscur de l'histoire ; cette place de choix attire aussi l'attention et la convoitise… des cybercriminels.

Et c'est là que le bât blesse : à l'heure actuelle, Bruxelles ne répond pas aux conditions requises pour en faire une capitale de la Cybersécurité. En cela, elle n'est pas encore mature. Cinq points illustrent et expliquent cet état de fait :

- Actions européennes intéressantes, mais floues,
- Action fédérale centralisée, mais peu de visibilité,
- Préoccupations régionales limitées aux instances publiques,
- Écart important entre l'offre de profils-métiers qualifiés belges et la demande de recrutement dû en partie aux manques de formation en Cybersécurité,
- Formations en Cybersécurité peu visibles sur le plan académique.

À l'avenir, ceci devra rapidement évoluer parallèlement aux besoins du secteur. Il sera intéressant d'ici quelques années de se poser à nouveau la question de la maturité de Bruxelles.

Sensibiliser, éduquer, réagir à la menace

3

- former une société de la sécurité -

3.1 La sensibilisation : pas une mince affaire

En 2010, 62,7% des citoyens belges ont été victimes de cybercriminalité[29]. Les attaques sont de mieux en mieux organisées et beaucoup de citoyens se laissent prendre au jeu. Dans ce contexte, sensibiliser devient un enjeu sociétal.

Il existe en Belgique une série d'initiatives et de campagnes de communication. On pense en premier lieu aux nombreuses conférences et *white paper*[30] que l'on voit fleurir partout sur le Net et dans le pays. Ces communications égrènent conseils de base, bonnes pratiques et guidelines de manière simplifiée. Elles s'adressent principalement à un public qui a fait la démarche de se renseigner sur le sujet et qui est arrivé sur le site ou la page de tel ou tel l'événement. Mais quid de ceux qui considèrent ne pas avoir besoin de sécurité ? Par quel moyen les sensibiliser ? Malgré la diversité des actions de communication, le citoyen se laisse difficilement convaincre. Selon M. Olivier Bogaert de la FCCU, « *on est dans une période charnière. Les mœurs vont évoluer. Il faut sensibiliser les enseignants et les parents pour qu'ils apprennent à leurs enfants les mesures de protection de base sur Internet* ».

On peut d'ailleurs s'interroger sur l'efficacité des campagnes de communication qui voient le jour sur le Net, dans la presse ou au travers de campagne publicitaires sur les réseaux d'affichage publics. Prenons l'exemple de la campagne « Take back the internet[31]» menée par le CCB en octobre 2016 afin de faire promouvoir la plateforme Safeonweb[32]. Selon eux, pendant la période de promotion publicitaire, le site web a été visité par 1 million et demi d'internautes, dont 88% pour la première fois. 200 000 visiteurs ont fait le test de sécurité. Une augmentation de 14% de mise en route de scan antivirus automatique sur les ordinateurs privés ou professionnels a été mesurée en réponse à cette campagne. Ces campagnes ont donc certes un impact positif de questionnement, mais les incidents sécuritaires sont toujours de plus en plus fréquents et cela pose une autre question : comment faire en sorte que les visiteurs adoptent une pratique responsable de sécurité au quotidien et non occasionnellement ? Il n'y a pas de mystère : il faut constamment répéter les mesures de protection afin d'en faire une habitude. « *Prenons l'exemple de la ceinture de sécurité dans les voitures. Combien de fois nos parents nous ont-ils répété de mettre notre ceinture dès que l'on monte dans la voiture ? Maintenant, en tant qu'adulte, après tant d'années, ce geste est devenu un acte normal, c'est devenu une évidence* », déclare M. Bogaert de la FCCU.

Dans ce cadre, le secteur public a un rôle à jouer, notamment en conseil et en accompagnement. « *Il doit pouvoir montrer l'exemple* », déclare M. Vautrin d'Innoviris. Il existe notamment des incubateurs d'entreprises, des projets tels qu'Impulse. Brussels[33] ou la plateforme d'information 1819[34] qui sont ouverts à tout créateur de start-up ou de petites entreprises dans le but d'accompagner et de conseiller.

29. http://www.lalibre.be/economie/digital/la-cybersecurite-est-un-enjeu-pour-tous-51b732d1e4b0de6db9756ab2
30. White paper : voir glossaire.
31. http://www.ccb.belgium.be/fr/news/r%C3%A9sultats-campagne-sensibilisation-2016
32. https://www.safeonweb.be/fr
33. http://www.abe-bao.be/fr
34. http://www.1819.be/fr/page/a-propos-de-1819

De plus, M. Gregorio Matias, de MCG insiste sur le fait qu'il « *faut personnaliser et diversifier les méthodes de communication pour les différentes cibles* ».
Quelles sont les solutions pour toucher et sensibiliser les différents publics ? Comment atteindre individuellement les publics différents : enfants, managers d'entreprises, employés, citoyens ? Le chantier est vaste…

3.2 Sensibiliser les entreprises

Comme le montrent les statistiques ci-dessous, le chiffre d'affaires des activités économiques dans le secteur IT belge se porte bien et ne cesse d'augmenter depuis 2013.

Indice du chiffre d'affaires par an, trimestre, et activité économique (NACE 2008) d'après les déclarations à la TVA

Année	2013	2014	2015	2016				2017
Trimestre				1er trim.	2eme trim.	3eme trim.	4eme trim.	1er trim.
	Indice brut	Indice brut	Indice brut	Indice brut	Indice brut	Indice brut	Indice brut	Indice brut
Niveau 1 - NACE 2008								
J62 Programmation, conseil et autres activités informatiques	115,64	125,75	137,15	142,45	142,8	132,46	168,59	150,02

Source : Chiffres d'affaires dans le secteur des services (selon la TVA). Direction générale Statistique - Statistics Belgium[35].

La question de la sécurité en entreprise nécessite deux distinctions au préalable.

1. Il y a deux types d'entreprises: des entreprises IT et les autres. Ces dernières, à l'instar des entreprises dont le *core business* est l'IT, recrutent énormément de profils dans l'informatique (par exemple les banques, les assurances, etc.) et sont donc d'importants fournisseurs de job en IT,
2. La sécurité n'a pas le même impact dans une grande société que dans une entreprise beaucoup plus petite du type PME, TPE ou start-up. Les moyens financiers sont différents, les ressources matérielles et humaines le sont également. Les communications vers ces deux catégories doivent être adaptées et séparées en deux axes : les grandes entreprises et les PME (et TPE).

3.2.1 Les grandes entreprises

Les grandes entreprises sont généralement déjà sensibilisées aux problématiques liées à la Cybersécurité. Souvent, les nombreuses données qu'elles manipulent ont une valeur économique importante. Dans le cas où le management est sensibilisé à la problématique, le danger vient souvent et aussi de manière involontaire d'un employé négligent. On note que le facteur humain est l'une des causes principales de brèches de sécurité dans les entreprises. Il y a donc également un travail de sensibilisation et de communication à destination des grandes entreprises à faire. Ce travail doit être effectué par l'entreprise qui doit se donner les moyens de valoriser une culture de la sécurité (*Cyber Security Policy*) auprès des employés. Des recommandations simples de bonne conduite et de prudence sont parfois suffisantes au bon fonctionnement d'une entreprise. Certaines entreprises testent occasionnellement leurs employés en les « piégeant ». Les employés qui se sont fait piéger sont par la suite accompagnés pour analyser leurs erreurs et sont invités à ne plus les rééditer dans la pratique. Toutefois, « *Cette pratique pose une question d'éthique. Dans ce cas, l'employé qui a fauté est pointé du doigt face à ses collègues et à l'entreprise* » dit M. Rousseaux de Digital Security. Il faut rendre anonymes les résultats. M. Pascal Van de Walle, CISO au CIRB confirme l'atout des tests dans les entreprises, mais insiste également sur l'obligation de rendre anonymes les répondants et précise que « *cela ne sert à rien de pointer les employés et leurs erreurs, il faut expliquer les raisons du problème et proposer des solutions* ». Des formations récurrentes sont

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

souvent nécessaires pour rappeler les règles de bonne utilisation des données. M. Rousseaux, lors de notre entrevue, insiste sur la notion de jeu pour sensibiliser. Dans son entreprise, Digital Security, une formule intéressante a été mise en place dans le cadre de leur prestation d'audit d'entreprise : La Red Team Attack[36] ! L'objectif est d'utiliser tous les moyens possibles (faux mails de l'entreprise, intrusion physique dans l'entreprise, etc.) pour contourner les protections de sécurité de l'entreprise. Cela finit généralement de manière amusante avec l'expert de Digital Security qui se prend en photo dans la salle des serveurs du client.

Il existe également sur le marché de la formation des outils de sensibilisation par le jeu : les Serious Games (jeux sérieux)[37]. Ces jeux simulent toutes sortes d'attaques permettant de voir la réactivité et les problèmes liés à la sécurisation d'une entreprise. Ils ont généralement pour cible les dirigeants d'entreprises.

Il est aussi intéressant de mentionner l'importance de la sécurité dès le recrutement. « *Pourquoi ne pas inclure, dès la signature du contrat, une Cyber Security Policy dans le règlement de travail ?* », déclare Jean-Marc André, fondateur d'UNIWAN. Et de poursuivre, « *cela permettrait à l'employé de comprendre dès le départ que l'entreprise tient à cœur la sécurité* ».

La sécurité concerne aussi et surtout les entreprises faisant partie des secteurs critiques : l'énergie, la mobilité, les télécoms, la finance, les assurances, la distribution d'eau potable, la santé publique, le gouvernement. Ces secteurs vitaux font l'objet d'une attention particulière dans la sécurité.

3.2.2 Les PME et TPE

Selon une étude de l'UCM[38] sur plus de 300 PME francophones, on constate que 88% des PME interrogées accordent de l'importance à la sécurité informatique de leur entreprise.

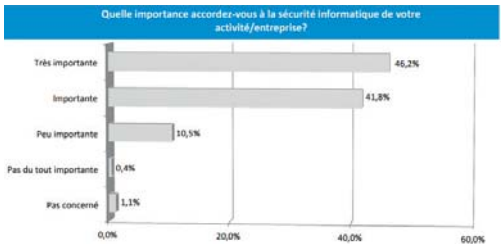


Figure 5 - Importance de la sécurité informatique - Étude UCM

D'ailleurs, 51% d'entre eux déclarent avoir déjà rencontré un problème de Cybersécurité (perte de données, piratage de messagerie, cryptage des données, paralysie temporaire, attaque du système informatique, etc.). 62,3% des sondés déclarent que la gestion de la sécurité est assurée par le patron, ou encore par une personne externe (par exemple une entreprise de consultance). Il est intéressant de noter que 1,6% des gens déclarent ne pas avoir besoin de moyens de sécurité.

Au final, quelles sont leurs attentes ? Ces attentes se concrétisent en trois priorités : répression plus forte du piratage informatique, baisse des coûts d'acquisition de certains outils et réduction/déduction fiscale sur les investissements de sécurisation de l'infrastructure informatique. Notons également que 45,8% d'entre eux aimeraient pouvoir bénéficier d'une formation aux bonnes pratiques.

L'étude se conclut par des recommandations aux pouvoirs publics :
- *Renforcement de l'investissement en matière de Cybersécurité favorisant les services de police pour le traitement des plaintes dans ce domaine ;*
- *Faire connaître plus encore les points de contacts et ressources existantes ;*

36. https://www.digitalsecurity.fr/fr/prestation-audit
37. Par exemple : https://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html ou 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

- *Sensibiliser aux bonnes pratiques via des modes de communication adaptée ;*
- *Développer des formations adaptées ciblées sur les problèmes que rencontrent les PME ;*
- *Intégrer la consultance en matière de sécurité informatique dans les dispositifs d'aide ;*
- *Faire connaître l'incitant fiscal fédéral en matière d'investissement en sécurité informatique et intégrer dans la liste des investissements éligibles les systèmes de sauvegarde de données adaptés aux indépendants ou PME,*[39] *…*

Pourtant, il est de notoriété publique que les PME et les TPE se sentent moins concernées par la sécurité informatique. « *Dans le cas des PME, il faut sensibiliser les têtes pensantes. Ne surtout pas faire peur, car cela ne résout rien, mais adapter sa communication aux managers*» déclare Gregorio Matias de MCG. Avant tout, il faut que l'entreprise fasse une évaluation de sa sécurité et se pose les questions suivantes :

- Qu'est-ce que je possède ? Qu'est-ce que je produis qui est à risque ?
- Est-ce que je manipule des données personnelles ?
- Est-ce que je manipule des données sensibles ?

C'est sur base de ces questions que l'entreprise peut décider de mettre en place une stratégie de la sécurité adaptée à la réalité.

Néanmoins, selon M. Ferdinand Casier, « *c'est une question de proportionnalité. Certaines toutes petites entreprises n'ont pas forcément besoin d'un arsenal de sécurité important* ».

Et pourtant, selon M. Valery Vander Geeten, Legal Officer au Centre pour la Cybersécurité Belgique, « *Les cibles des attaques sont de plus en plus souvent des PME* ». On constate ce changement depuis quelque temps. Avant, les pirates concentraient leurs efforts sur les grandes compagnies qui ont désormais les moyens humains, financiers et technologiques de se prémunir des cyberattaques. Ce n'est pas le cas de toutes les PME. Elles n'ont pas les mêmes moyens ni la même prise de conscience face au phénomène de hacking[40]. Il arrive même régulièrement que des bases de données de sociétés soient visitées par des pirates informatiques sans laisser de traces.

Selon M. Vincent Defrenne de NVISO, « *Les PME disposent rarement de la masse critique et des compétences pour faire face à ces problèmes* ». Le problème lié aux PME se distingue en trois points distincts :

- La **fragmentation** sur le territoire belge est énorme : il est difficile de toucher toutes les entreprises.
- La **récurrence** : les PME réagissent différemment face à la Cybersécurité. Quand elles sont impactées par un problème en lien avec la Cybersécurité, elles réagissent pour trouver une solution, mais elles n'agissent pas préventivement.
- La **maturité** n'est pas encore là : les PME ne comprennent pas ce qu'on leur propose en termes de solutions Cybersécurité.

On doit donc s'adresser aux petites et moyennes structures avec une communication adaptée. Souvent, dans ce type de structure, la Cybersécurité n'est pas la priorité. En effet, selon M. Nicolas Vautrin, Team Leader - Recherche Industrielle et Innovation chez Innoviris, « *la plupart des petites entreprises n'ont pas les moyens d'engager un expert en Cybersécurité* ». C'est aussi le cas pour les start-ups qui veulent lancer leur projet le plus rapidement possible. La sécurité est la dernière étape, souvent négligée. Ainsi, il est impératif que le secteur public

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

se donne un rôle à jouer dans l'accompagnement et la sensibilisation des PME. Une fois les directions managériales sensibles aux problèmes de la sécurité, la première étape est franchie. La suite consiste à mettre en place une politique de sécurité qui pourra être appliquée au sein de leur entreprise. Vis-à-vis de ce public, des recommandations trop générales sont inefficaces et pour l'instant la sensibilisation porte peu ses fruits. Il faut trouver une communication personnalisée mettant en valeur l'importance de la sécurité avec des cas concrets.

Une solution pour ces petites structures serait d'engager un profil aux connaissances plus générales (par exemple : un administrateur réseau) qui pourrait suivre une formation courte lui permettant d'avoir des notions en sécurité. Une autre solution : Il est courant pour ces sociétés de faire appel à des ressources externes pour assurer la sécurité des infrastructures. Les entreprises s'associent généralement avec des agences de consultance qui proposent des services adaptés aux besoins de la structure. Il est important de noter que ces agences de consultance doivent aussi mettre à jour leurs connaissances en matière de Cybersécurité. Ainsi, c'est aussi vers ces acteurs qu'il faut diriger des campagnes de sensibilisation.

3.3 Le rôle des médias

Dans cette course à la sensibilisation, les médias pourraient jouer un rôle important d'éducation. Les grandes menaces informatiques sont de plus en plus médiatisées. Il ne se passe pas une semaine sans qu'un nouveau virus, campagne de ransomware, ou autre type d'attaques informatiques ne soient dévoilés au grand jour. Elles sont encore plus médiatisées si elles sont parvenues à atteindre une grande entreprise ou une grande institution. Néanmoins, il faut rester prudent avec le rôle de la presse. « *La plupart du temps, les médias amplifient un événement, mais ne l'expliquent pas* », déclare Gregorio Matias. Les médias jouent avec le phénomène de la peur afin de vendre plus facilement leur contenu. Gregorio Matias insiste sur le fait que « *la peur n'est pas la solution pour parler de ce genre de phénomène, ce qui est malheureusement souvent le fonds de commerce de la presse* ». Cela ne fait pas avancer les choses. Il faut pouvoir sensibiliser le grand public par l'explication et l'éducation et non par la peur.

3.4 La formation en entreprise : une solution ?

Nous l'avons remarqué, sensibiliser les différents publics n'est pas chose facile. Dans ce sens, la formation est un bon moyen de propager l'information. Elle peut s'adapter aux profils différents et aux différents besoins.

Il existe des structures qui organisent des formations dans les entreprises pour sensibiliser le management et les employés. Ces formations peuvent être prises en charge par l'équipe informatique de l'entreprise ou par une agence externe spécialisée dans la formation en sécurité.

Il est également important de sensibiliser les plus jeunes à la sécurité informatique. Or, actuellement, il existe peu de formations de sensibilisation destinées aux enfants. Un enfant conscient de sa sécurité sur le Net sera probablement un adulte et un employé qui applique déjà naturellement les mesures de base de sécurité. Dans notre monde en perpétuel mouvement où le progrès informatique est de plus en plus rapide, qu'attend-on pour mettre en place des cours d'informatique et de sensibilisation au monde du virtuel dans les écoles ? Pourtant, il existe des initiatives très complètes pour sensibiliser, comme celle de Child Focus: clicksafe[41] qui offre des formations et toute une série d'outils pédagogiques[42] à destination des professionnels et des parents. Elles sont cependant peu présentes sur le marché et manquent de visibilité.

41. http://www.childfocus.be/sites/default/files/manual_uploads/fiche_p_1_e-safety_pour_professionnel2.pdf
42. http://www.childfocus.be/fr/prevention/clicksafe-tout-sur-la-securite-en-ligne

4 Les métiers de la Cybersécurité

4.1 Le problème de l'offre et de la demande

Il y a encore une dizaine d'années, les profils-métiers liés à la Cybersécurité n'avaient pas la même importance qu'aujourd'hui. Nous constatons depuis quelques années une explosion des recrutements. Les métiers de la sécurité sont en pleine émergence. Cette mutation est influencée par plusieurs facteurs :

- La médiatisation des attaques de grande envergure,
- Les besoins grandissants des entreprises en Cybersécurité,
- La constitution de mesures européennes apportant des besoins jusqu'à aujourd'hui inexistants de structuration sécuritaire au sein des entreprises.

Les études actuelles estiment que d'ici 2020, la Belgique sera en manque de 2000 experts en Cybersécurité[43]. À titre d'exemple, lors de l'été 2017, la Défense a déclaré développer la Cybersécurité en engageant 200 experts d'ici la fin de l'année[44]. Les acteurs de la ville de Bruxelles comme le CIRB envisagent encore de recruter plusieurs CISO (*Chief Information Security Officer*) afin de se préparer aux mesures émanant du GDPR (*General data protection reglementation*). Le constat est frappant : il y a un écart entre l'offre de profils-métiers sur le marché de l'emploi et la demande de recrutement des entreprises bruxelloises.

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 Définir les indicateurs des métiers de la Cybersécurité

Les profils-métiers associés à la Cybersécurité sont divers et variés. Comme dans beaucoup de domaines informatiques, les dénominations sont parfois nombreuses et leurs définitions floues.

Actuellement, en Belgique, il n'existe aucun référentiel universel qui permette de classifier les métiers liés à la sécurité informatique. Ainsi, les caractéristiques de ces postes sont imprécises. Il est difficile de s'y retrouver dans ces conditions.

Lors de la phase de préparation de ce rapport, nous avons visité plusieurs sites de recrutement afin d'analyser les descriptions de profils-métiers ; Actiris[45], LinkedIn[46], le site du Selor[47], ICTJOB[48], etc. Nous avons analysé plusieurs annonces de recrutement dans le privé et le secteur public.

Que peut-on dire de ces dénominations de profils trouvés au fil de nos recherches ? D'abord, que la multitude des titres de fonction pousse à la confusion.

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/fr-BE/Offres-d-emploi.aspx
46. https://www.linkedin.com/uas/login
47. http://www.selor.be/fr/
48. https://www.ictjob.be/fr/?cid=SEAdvert_Google_Search_FR_Brand-BE-FR_c_B02.01)-Exact_ictjob_FP_-_

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. Les dénominations de fonction dans la Cybersécurité sont trop nombreuses.

En 2014, une étude française du CEIS[49] (Conseil Européen d'Intelligence Stratégique) définit les éléments clés des fonctions liées à la Cybersécurité[50]. Le rapport indique pour chaque métier des indicateurs avec trois types de densités :

- **La densité IT** : cette densité englobe la technicité du métier (l'aspect purement informatique) qui est de loin la densité la plus importante. Elle comprend la veille, le support, la maintenance, etc.
- **La densité sécurité** : La culture sécurité qui comprend l'aspect marketing, gestion des risques, etc.
- **La densité métier** : La connaissance du domaine d'application et de l'environnement professionnel. La densité métier regroupe des attributs tels que l'aspect juridique, la compliance[51], la recherche de vulnérabilités.

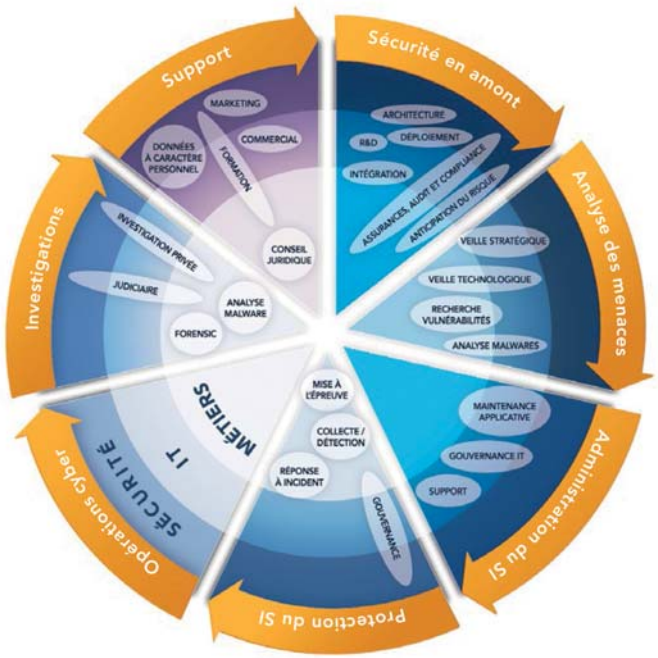


Figure 6 - Référentiel des Métiers selon leur densité -
Source : Quel référentiel pour les métiers de la Cybersécurité ?

Au vu, de ces référentiels, nous mettons en lumière plusieurs mots clés que l'on associe de préférence aux métiers de la Cybersécurité :

1. La communication (précédée de la veille),
2. La stratégie,
3. L'analyse du risque,
4. L'adéquation juridique.

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 : voir glossaire.

4.3 Frost & Sullivan : une étude des métiers à travers le monde

Une étude de Frost & Sullivan[52] analyse la situation du métier de cyber spécialiste dans le monde. L'étude constate qu'il y a un écart grandissant entre l'augmentation des menaces virtuelles et le recrutement de travailleurs dans la Cybersécurité. En Europe, seuls 66% des postes sont pourvus. Les raisons principales de ce problème de recrutement sont la difficulté à trouver des personnes qualifiées (48%), le manque de compréhension du problème de la sécurité par la direction (41%), le manque de budget pour le recrutement d'un membre du personnel en plus (39%), etc. Néanmoins, l'étude souligne la volonté au sein de l'Europe d'accroître le recrutement de 20% et plus.

L'étude de Frost & Sullivan s'intéresse aussi au background des professionnels de la Cybersécurité. Nous constatons à travers les chiffres que 24% des spécialistes en Europe sont issus d'un parcours différent, pas forcément en lien avec l'IT ou l'ingénierie (qui sont des filières classiques pour atteindre un poste dans la sécurité). Ces 24% proviennent principalement du secteur lié au business, du secteur du marketing, de la finance et du secteur militaire.

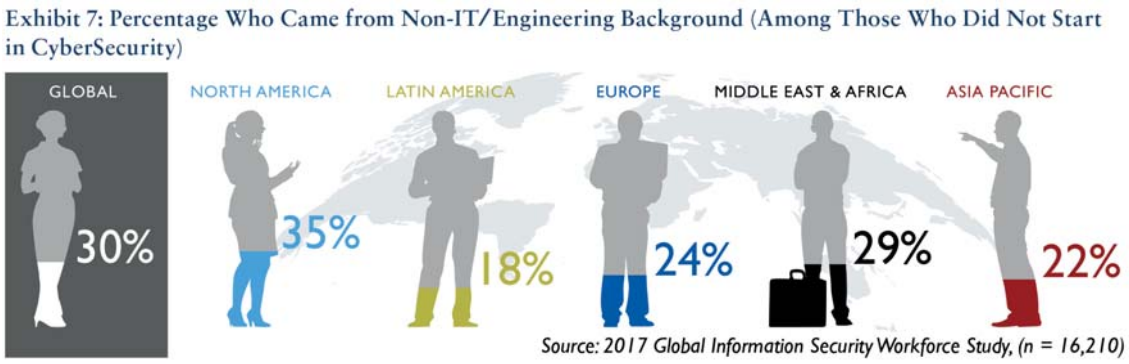
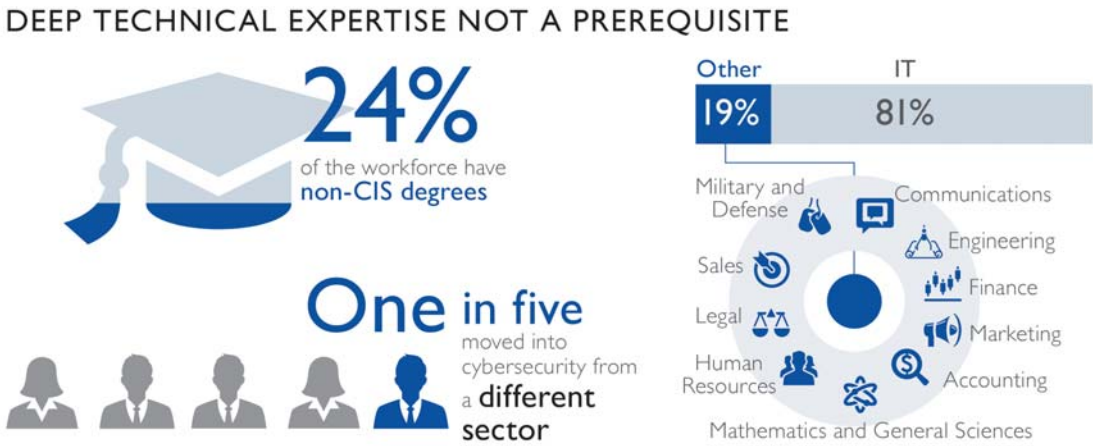


Figure 7 - Profils issus de filières Non IT
Source : https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf



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

4.4 L'impact des réglementations européennes sur les métiers

L'arrivée de nouvelles réglementations européennes destinées à réglementer la Cybersécurité a et aura un impact percutant sur les métiers IT et le mode de recrutement. Il est de plus en plus nécessaire de donner un cadre légal à la protection des données et des infrastructures.

Jusqu'à présent, il n'existe quasiment qu'une seule réglementation imposée. Il s'agit de la directive « *vie privée* ». Elle a été mise en place en 1998 et légifère notamment sur le transfert des données entre l'Union Européenne et les États-Unis.

Cependant, il existe d'autres mesures plus directement liées à la gestion des données privées et à la Cybersécurité que nous allons présenter dans ce rapport.

Il s'agit de deux mesures européennes qui ont un impact direct sur la question de la Cybersécurité : la directive NIS et le GDPR.

4.4.1 Network and Information Security - NIS

La directive « *Network and Information Security* » est entrée en vigueur en juillet 2016. Cette directive est destinée à assurer un « *niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne* »[53]. Cette mesure est généralement cumulative avec le règlement sur la protection des données (GDPR) que nous allons présenter ci-après.

Cette mesure a eu des implications sur la Belgique[54] à travers deux objectifs :

1. Définir une nouvelle stratégie nationale en matière de Cybersécurité et mettre en place des cadres réglementaires ;
2. Créer le Centre pour la Cybersécurité[55] qui est l'autorité nationale compétente.

La mesure NIS s'applique uniquement pour certaines entreprises.

1. Les opérateurs de services essentiels dans certains secteurs : énergie, banque, santé, infrastructures numériques, transport, etc. …
2. Les fournisseurs de service numériques.

4.4.2 General Data Protection Regulation - GDPR

Le GDPR, *General Data Protection Regulation*, est un règlement européen légiférant sur la protection des données. Ce règlement impacte toutes les entreprises traitant et stockant des données. Autant dire qu'au contraire de la directive NIS, cette mesure concerne la quasi-totalité des entreprises.

Art. 16, §4 de la loi du 8 décembre 1992

La GDPR peut être considérée comme la continuité de la loi du 8 décembre 1992 qui dit :

« *Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant, doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel*[56] ».

« *Ces mesures doivent assurer un niveau de protection adéquat, compte tenu ;*
1. De l'état de la technique en la matière,

53. http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2013/0027(COD)
54. http://www.1819.be/fr/blog/nouvelle-directive-europeenne-cybersecurite-impact-pour-les-entreprises
55. http://www.ccb.belgium.be/fr
56. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992120832&table_name=loi

2. Des frais qu'entraîne l'application de ces mesures,
3. De la nature des données à protéger,
4. Des risques potentiels […][57] »

Dans les grandes lignes, les obligations du GDPR[58] sont de :
1. Nommer un délégué de la protection des données (DPO),
2. Obliger l'adoption de sécurité renforcée,
3. Obliger l'analyse d'impact,
4. Créer un registre des activités de traitement.

Cette mesure prendra effet dès mai 2018 et apportera son lot de sanctions dans les cas où la mesure n'est pas appliquée correctement.

Le GDPR est la principale raison des recrutements massifs des personnes ayant un profil-métier proche du DPO (Data Protection Officer). La deadline de la mise en exécution du GDPR accélère et influence donc la hausse des recrutements dans les entreprises.

4.5 Problème d'image et mixité au cœur du problème

Les métiers de la Cybersecurity souffrent d'une image stéréotypée. La plupart du temps, quand nous imaginons une personne qui travaille dans la Cybersécurité, on imagine un « geek » encapuchonné à l'air peu recommandable, enfermé dans une pièce sombre remplie d'écrans et pianotant frénétiquement sur son clavier avec l'objectif de pirater les systèmes informatiques d'une grande entreprise. La presse n'aide pas à casser ce cliché tenace qui ne rend pas le job attirant. De plus, certains profils-métiers comme le *Pentester*[59] (nous présentons de manière plus approfondie ce profil dans la partie « 4.7 Focus sur trois profils-métiers en Cybersécurité ») sont actuellement considérés comme illégaux en Belgique. En réalité, les profils en Cybersécurité sont très demandés sur le marché de l'emploi et requièrent également des *softs skills* particuliers :

- Des dispositions à la communication et à l'éducation,
- De la créativité, une bonne intuition,
- De grandes capacités de recherche,
- Une passion pour l'apprentissage,
- Le sens du jeu et du défi.

Dans l'article « la guerre des talents en *Cybersécurité*[60] », Koen Maris, Chief technology officer Cyber Security chez Atos Benelux & The Nordics, affirme que « *la Cybersécurité est un état d'esprit, pas une formation* ». En effet, les compétences techniques, informatiques sont une chose, mais l'expertise en Cybersécurité requière une série de capacités énumérées précédemment que tous les informaticiens ne peuvent avoir.

Dans une étude de Frost and Sullivan, il est aussi intéressant de noter que le pourcentage de présence des femmes[61] dans les fonctions en lien avec la sécurité est assez bas. 7% en Europe, 14% en Amérique du Nord, 9% en Afrique et 10% en Asie[62]. Ces chiffres peinent à augmenter et posent question étant donné que les femmes recrutées dans la Cybersécurité sont 50% à

57. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992120832&table_name=loi
58. GDPR et NIS, quelle(s) obligation(s) de sécurité ? Franck Dumortier, CRIDS [en ligne] 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

posséder un niveau supérieur de master voir plus contre 45% pour les hommes[63]. Néanmoins, il n'est pas rare de découvrir chez elles, un parcours atypique au contraire des hommes qui sont généralement issus de filières classiques (comme l'informatique, l'ingénierie, etc.). Néanmoins, certains profils-métier, comme celui du pentester, se distinguent des statistiques générales présentées précédemment. Nous analysons le profil du pentester dans la partie 4.7 focus sur trois profils métiers en Cybersécurité.

Toujours pour la problématique de la mixité, nous présentons un projet intéressant : Cyber Wayfinder[64]. Cette initiative vise les femmes qui veulent travailler dans le domaine de la Cybersécurité. L'objectif de Cyber Wayfinder est de créer une communauté belge de femmes expertes de la Cybersécurité et de construire un réseau d'entreprises qui ont besoin de profils qualifiés. Ce programme s'articule autour d'une série de Bootcamp et de cours organisés par l'école de coding Le wagon[65] à Bruxelles.

4.6 Méthodes de recrutement : Nécessité d'évoluer ?

La Belgique manque d'experts en Cybersécurité, c'est un fait. Malgré les nombreuses formations émergentes, la demande d'experts n'est toujours pas satisfaite. Beaucoup de spécialistes viennent de l'étranger, car ils sont souvent plus formés et plus nombreux, tout simplement.

La problématique de la présence d'un expert de la sécurité des données amène à se poser la question sur les modes de recrutement. En 2017, le rapport de Frost & Sullivan[66] estime qu'en vue des caractéristiques des métiers de la Cybersécurité (manque de recrutement féminin, profils issus de background autres que l'IT), les méthodes de recrutement doivent être actualisées. Le rapport suggère d'écarter le critère de l'expérience professionnelle étant donné le nombre croissant d'employés issus de domaines non traditionnels qui s'adaptent rapidement aux compétences et exigences du métier. Il ne faut pas négliger l'importance des softs skills dans ce métier. Les méthodes de recrutement actuelles créent des barrières alors que la sphère professionnelle a tant besoin de recruter.

Beaucoup d'entreprises ne placent pas la sécurité au top de leurs priorités et n'ont pas les ressources financières pour engager une nouvelle personne à cet effet. Même si les entreprises doivent mettre en place des mesures de sécurité, le recrutement d'expert n'est pas nécessaire. D'autres possibilités sont envisageables : former un membre du personnel à la sécurité ou faire appel à des agences de consultance spécialisées dans la Cybersécurité.

Quoi qu'il en soit, les demandes de recrutement sont de plus en plus nombreuses et émanent souvent de grandes entreprises ou d'organisations gouvernementales. Les autres entreprises reconvertissent un ou plusieurs de leurs employés (souvent des informaticiens) ou décident de se tourner vers de la consultance externe.

4.7 Focus sur trois profils-métiers en Cybersécurité

4.7.1 Le CISO

Le *Chief Information Security Officer* (CISO) ou RSSI (*Responsable de la sécurité des systèmes d'information*) est l'EXPERT de la sécurité à proprement parler. Souvent cité dans les débats sur la Cybersécurité, c'est lui qui aide son entreprise à atteindre le niveau de sécurité défini

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

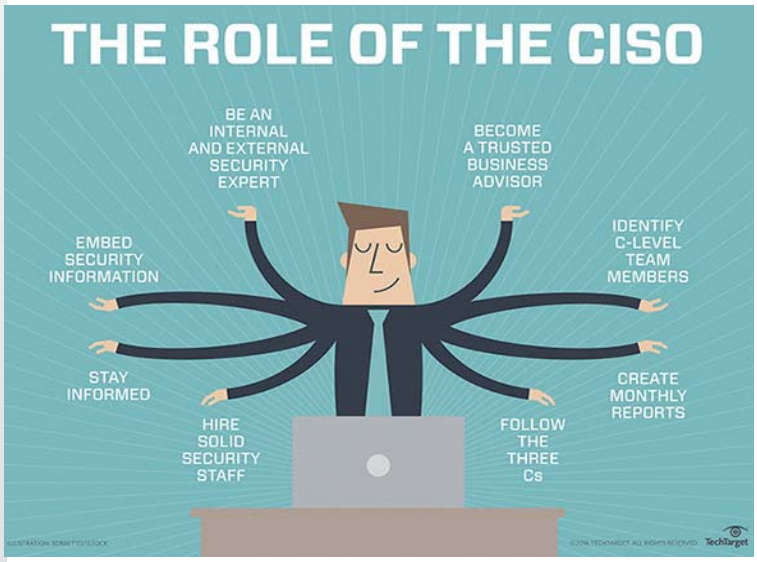


Figure 8 - Le rôle du CISO
source : SearchSecurity : http://searchsecurity.techtarget.com/definition/CISO-chief-information-security-officer

et à le garder[67]. C'est le profil clé qui intervient en cas d'attaque informatique, mais c'est aussi celui qui met en place la stratégie préventive pour éviter les problèmes. Il veille à ce que les réseaux et infrastructures soient suffisamment sécurisés. Ce profil se situe dans la hiérarchie de l'entreprise entre le management et les employés et fait figure d'intermédiaire sur la question de la sécurité. Il établit des consignes techniques (mise en place de pare-feu, mises à jour, etc.) et définit les règles de « bonne conduite » dans le but d'adopter durablement une culture de la sécurité en entreprise. Il a donc une bonne connaissance en sécurité, en administration réseau (il maitrise notamment la norme ISO 27000), mais également en Risk Management (gestion des risques). Il sait communiquer avec la direction, mais également avec les employés ou les clients. Il doit également avoir une bonne vision du cadre juridique et des mesures sécuritaires qui régissent son métier.

L'essentiel de ses journées est consacré à la résolution de problèmes liés à la sécurité en entreprise. Il consacre également beaucoup de temps à communiquer avec ses collègues et à rappeler les consignes de sécurité. Il s'assure que son entreprise remplisse les conditions pour respecter les diverses règles et mesures européennes. « *Ils assument les rôles de stratège, communicant, expert, influenceur et manager* ». Cette phrase, issue du site SPSearch Promoteur de talents[68], résume très bien la complexité du rôle de Chief Information Security Officer. Son rôle requiert trois caractéristiques : autorité, indépendance et responsabilité[69].

Le CISO est la plupart du temps un universitaire. Il a fait des études en informatique et ingénierie, avec une spécialisation en sécurité. Sa qualité d'expert et son rôle stratégique dans l'entreprise demandent une certaine expérience dans le domaine de la sécurité. C'est pourquoi la plupart des annonces publiées pour ce poste demandent un profil de haut niveau avec plusieurs années d'expérience dans le domaine.

Nous analysons généralement ce métier à l'échelle d'une grande entreprise ou institution qui a les moyens (financiers, humains et priorité stratégique) d'engager un CISO. Dans le cas des plus petites entreprises, c'est souvent un gestionnaire du parc informatique qui porte la casquette de Monsieur Sécurité. On parle aussi d'externalisation de la fonction pour les sociétés de type PME[70]. Ces entreprises font ainsi appel à des sociétés de consultance qui gèrent le parc informatique de l'entreprise avec ses aspects sécuritaires.

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/
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%3Dcles-de-smartcity-brussels
70. https://www.ysosecure.com/securite-information/role-rssi.html

LES COMPÉTENCES TECHNIQUES GÉNÉRALEMENT DEMANDÉES À UN CISO

- CompTIA Security+
- GSEC: GIAC Security Essentials Certification
- SSCP: Systems Security Certified Practitioner
- CISSP: Certified Information Systems Security Professional (certificat orienté polices et gestion de la sécurité),
- CISA: Certified Information Systems Auditor en particulier pour les auditeurs,
- CISM: Certified Information Security Manager, orienté management, par exemple pour le CIO,
- GCIH: GIAC Certified Incident Handler (pour le gestionnaire d'incidents; tout ce qui touche la détection, la gestion d'incidents liés à l'informatique),
- CEH: Certified Ethical Hacker,
- OSCP: Offensive Security Certified Professional,
- Stratégie IT, architecture et sécurité d'entreprise,
- Concepts de sécurité autour du DNS, le routing, l'authentification d'utilisateurs et de machines, la VPN, les services proxy et les technologies DDOS,
- ISO 27002, ITIL et framework COBIT,
- Les checklists compliance (homologation) PCI, HIPAA, NIST, GLBA et SOX,
- Windows, UNIX et système d'exploitation Linux,
- C, C++, C#, Java et/ou PHP
- Protocoles pare-feu et de détection / prévention d'intrusion
- Pratiques de codage sécurisé, piratage éthique et modélisation des menaces TCP/IP, réseau, routing et switching,
- Développement et définition d'Architecture sécurité réseau,
- Connaissance d'outils et de méthodologies d'auditing et d'évaluation des risques liés au Cloud

4.7.2 Le DPO

Le Data Protection Officer est le « chef d'orchestre de la conformité[71] ». Ce profil-métier connait son émergence en raison de la mesure du GDPR qui rend obligatoire la présence d'un DPO dans toutes les administrations.
Qui est le DPO ? C'est celui qui valorise les données et qui établit les règles d'utilisation. La société peut engager ou nommer un employé au poste de DPO ou faire appel à un consultant externe en DPO.

Au contraire du CISO, le DPO n'a pas nécessairement des compétences expertes en Cybersécurité. Il doit cependant avoir une solide culture juridique et informatique[72]. Il doit être un bon gestionnaire de projet et avoir un bon sens de la communication. C'est lui qui fait adopter des mesures préventives de sécurité des données, mais aussi qui doit gérer rapidement les situations de crise. Le DPO s'assure que le concept du « Privacy by design[73] » soit appliqué.

71. 72. Le métier de Data Protection Officer (DPO), obligatoire dès 2018 dans de nombreuses entreprises, Blog du Modérateur [en ligne] https://www.blogdumoderateur.com/metier-data-protection-officer-dpo/
73. Privacy by design : voir glossaire.

Figure 9 - Infographie : Le métier de Data Protection Officer source image http://www.abilways-digital.com

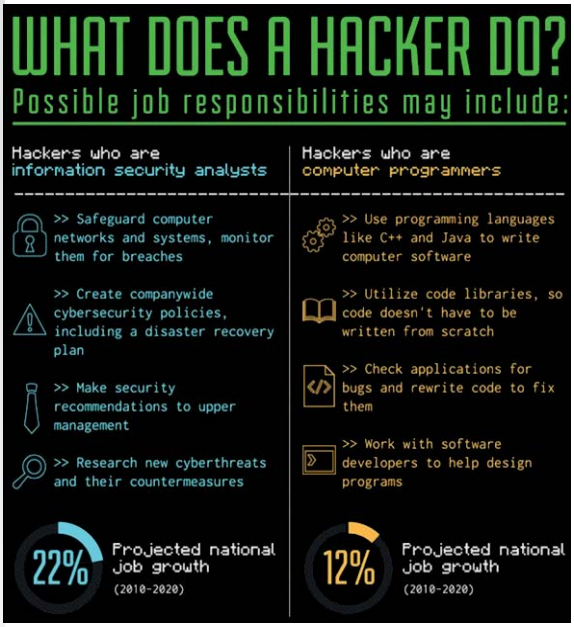


Figure 10 - What does a hacker do? https://fossbytes.com/how-to-become-a-ethical-hacker/

Il s'agit d'intégrer la protection des données dès la conception et le fonctionnement du système ou du réseau informatique. Il est également le responsable de la sensibilisation en élaborant un guide des bonnes pratiques pour travailler en toute sécurité. C'est l'employé clé qui est consulté sur les sujets liés à la protection des données privées[74].

Il travaille en collaboration avec le CISO et la direction. Il joue l'intermédiaire avec les employés et doit communiquer sur les mesures de sécurité à adopter.

En général, le DPO est détenteur d'un master parfois en informatique, mais ce n'est pas une nécessité. Il a souvent suivi des formations complémentaires ou obtenu des certifications (des exemples de formations DPO sont abordés dans le chapitre sur la formation) pour atteindre le poste de délégué de la protection des données.

4.7.3 Le « hackeur éthique »

Le « hackeur éthique » est le chercheur en sécurité informatique qui collabore avec des organisations (entreprises privées, asbl ou entités publiques) pour détecter des vulnérabilités dans leurs systèmes ou réseaux informatiques.

Avec l'autorisation de l'organisation concernée, il se met à la place d'un pirate informatique (hackeur) et teste les systèmes informatiques de cette organisation. Il doit pour cela respecter strictement le contenu de la politique de divulgation coordonnée des vulnérabilités (en anglais, « coordinated vulnerability disclosure policy ») ou d'un programme de récompenses des vulnérabilités (en anglais « vulnerability rewards program » ou «bug bounty program») de l'organisation responsable du système informatique.

Selon la définition donnée par le CCB, une politique de divulgation coordonnée (ou «politique de divulgation responsable») des vulnérabilités est un ensemble de règles préalablement déterminées par une organisation responsable de technologies de l'information ou de la communication autorisant des chercheurs en sécurité ou le grand public à rechercher, avec de bonnes intentions, de potentielles vulnérabilités dans ses

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/

systèmes, ou à lui transmettre toute information pertinente découverte à ce sujet. Ces règles, généralement rendues publiques sur un site internet, permettent de fixer un cadre juridique à la collaboration entre l'organisation responsable et les participants à la politique.

Bien que la notion évoque explicitement la « divulgation » de la vulnérabilité, celle-ci ne constitue pas une condition nécessaire à la réalisation d'une politique de divulgation coordonnée. En réalité, il ne s'agit que d'une modalité facultative qui peut être librement choisie ou non par les parties, au contraire de l'autorisation donnée d'accéder aux systèmes de l'organisation responsable.

La politique de divulgation coordonnée des vulnérabilités constitue, à ce titre, une forme de contrat d'adhésion dans lequel toutes les dispositions contractuelles sont fixées par l'organisation responsable et ensuite acceptées par le chercheur en sécurité lorsque celui-ci décide librement de participer au programme mis en place.

Quant au programme de récompenses des vulnérabilités, il vise l'ensemble des règles définies par une organisation responsable pour octroyer des récompenses aux chercheurs en sécurité ou au grand public qui identifieraient des vulnérabilités dans les technologies qu'elle utilise. Cette récompense peut prendre la forme d'une somme d'argent, de cadeaux ou d'une simple reconnaissance publique.

Pour autant que les dispositions légales soient respectées (conditions de l'autorisation accordée par l'organisation, autres dispositions pénales, le secret des communications électroniques et la protection des données à caractère personnel), le hacking éthique est parfaitement légal en Belgique.

En 2018, le CCB devrait rendre public un Guide sur les politiques de divulgation coordonnée des vulnérabilités en Belgique. Ce guide comprendra une partie sur les bonnes pratiques (avec un modèle de politique) et une autre partie sur les aspects légaux.

Les caractéristiques du hackeur éthique sont : la curiosité, l'indépendance, la capacité à « sortir du cadre[75] » et à se mettre à la place d'un hackeur pour agir comme lui. Il est capable de détecter les problèmes et de proposer des pistes d'amélioration. Appelé aussi « pentesteur » (contraction du terme « penetration tester[76] »), il est capable d'identifier les points d'entrée possibles, d'effectuer des tentatives d'intrusion et de documenter des résultats[77]. Le Hackeur éthique a le sens du jeu et du défi. Chaque projet est pour lui l'occasion de démontrer aux clients que leur entreprise n'est pas invulnérable. Son objectif est de trouver la moindre porte d'entrée dans l'infrastructure de l'entreprise (informatique ou intrusion physique) pour rapporter au client les points sensibles et lui proposer des améliorations. (Par exemple, nous avons déjà présenté la société Digital Security et sa technique spéciale d'Audit : la Red Team Attack[78]).

Même s'il n'existe pas encore de formation à proprement parler sur le sujet, certains masters abordent le sujet, mais de manière volontairement floue. C'est un métier que l'on apprend dans des formations complémentaires (*Certified Ethical Hacker* « CEH »)[79] ou dans des universités étrangères. On peut notamment présenter la *licence professionnelle des collaborateurs pour la défense et l'anti-intrusion des systèmes informatiques (CDAISI)*[80] à Maubeuge en France. Cette formation forme au métier de « *Pentesteur* ».

75. http://www.orange-business.com/fr/blogs/securite/securite-organisationnelle-et-humaine/conseils-pour-devenir-un-hacker-ethique-osd14
76. Penetration tester : voir glossaire.
77. http://www.pentesteur.com/pentesteur-ethical-hacking
78. Voir chapitre 3.2 : sensibiliser les entreprises, 3.2.1 Les grandes entreprises.
79. Howest, Hogeschool West-Vlaanderen
80. http://www.univ-valenciennes.fr/IUT/lecole-des-hackers-maubeuge

5 Paysage de la formation Cybersécurité à Bruxelles

Il existe en Belgique une série de formations enseignant la sécurité informatique sur plusieurs niveaux. Ces formations répondent à un besoin grandissant de spécialistes de la Cybersécurité. On en trouve pour tous les goûts : masters, bacheliers, spécialisations, certifications, formations continues, etc. Dans ce rapport, nous allons nous concentrer sur le paysage bruxellois[81]. Le problème actuel est que la plupart des formations ne sont pas en connexion avec les problèmes de terrain et négligent souvent l'importance des compétences dites « soft skills » liées à la Cybersécurité et pourtant essentielles. Les cours de Cybersécurité figurent généralement dans les cursus informatiques, d'ingénierie, de gestion (management) et juridiques.

Le paysage académique commence à prendre conscience du besoin de profils en Cybersécurité. Une série de formations commence à se développer sur Bruxelles pour répondre à tous les besoins. C'est une bonne nouvelle pour les perspectives de recrutement. Une liste complète de toutes les formations données en Cybersécurité à travers la Belgique est disponible sur le site du CCB[82].

5.1 Les formations universitaires

5.1.1 Master en Cybersécurité (ULB, UCL, UNamur, ERM, HELB, ESI-HEB)[83]

L'Université de Namur, l'Université libre de Bruxelles, l'Université Catholique de Louvain, la Haute École Libre de Bruxelles, La Haute École Bruxelles-Brabant (ESI) et l'école royale militaire se sont associées pour construire ce master. Répartis sur deux ans, les cours se déroulent sur trois campus à Bruxelles, à Louvain et à Namur.

Les domaines abordés sont les suivants :

- Cryptographie et cryptanalyse,
- Réseaux de télécommunications et informatique distribuée,
- Sécurité de l'information et sécurisation des systèmes informatiques,
- Techniques de gestion et d'exploitation de métadonnées, inférence et fuites d'information
- Forensique[84] et investigation,
- Gestion de la sécurité et mise en œuvre de normes, audits et politique de sécurité,
- Aspects légaux, éthiques et humains de la sécurité,
- Conception d'architectures de systèmes sécurisés,
- Méthodes de génie logiciel et de développement sécurisé.

Hormis les compétences purement techniques, ce master prend en compte les demandes que l'on a pu dégager dans les offres de recrutement. Rappelons ces mots clés importants : la communication (précédé de la veille), la stratégie, l'analyse du risque, l'adéquation juridique. Étant donné que le spécialiste de la sécurité doit avoir des compétences d'informaticien, de manager et d'informateur, il est nécessaire que ces éléments soient pris en compte dans ce master, surtout s'il s'échelonne sur deux ans.

81. Cette liste est exemplative et évolutive et ne se veut en aucun cas exhaustive.
82. http://www.ccb.belgium.be/fr/ict-security-education-belgium
83. https://masterincybersecurity.ulb.ac.be/
84. Forensique : voir glossaire

La formation est accessible aux détenteurs d'un bachelier en informatique ou ingénierie et l'étudiant doit donc avoir un profil d'informaticien.

Ce cursus peut être également utilisé par des informaticiens cherchant à acquérir des connaissances poussées dans la sécurité, et faire ainsi une spécialisation après plusieurs années d'expérience dans le monde du travail.

5.1.2 Information security management education – Solvay Brussels School (ULB)[85]
Cette formation se décline en deux formules.
Tout d'abord, un master de 288 heures de cours qui comprend l'entièreté des modules de cours :

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

Ensuite, trois programmes personnalisables qui comprennent 144 heures de cours :

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

Cette formation est destinée à des managers et non à de purs informaticiens même si le module axé sur la sécurité est automatiquement présent dans tous les programmes. Ce module permet entre autres d'acquérir des compétences managériales et comportementales : prévention, réponse à un risque, apprentissage de technologies associées à la Cybersécurité.

5.2 Des cours en Cybersécurité à l'université

Il est fréquent de découvrir des cours en lien avec la Cybersécurité dans des formations plus classiques (ingénierie, informatique, etc.). Cette intégration permet aux futurs diplômés de comprendre et d'intégrer la problématique de la Cybersécurité dans leur métier.
Nous allons analyser rapidement quelques-uns de ces cours.

Protocols, cryptanalysis and mathematical cryptology - ULB. Ce cours est délivré dans le programme de sciences informatiques ou pour les ingénieurs civils en informatique. Il permet notamment « d'initier aux méthodes et attitudes spécifiques en recherche en cryptologie et d'assimiler les principaux résultats de cryptanalyse moderne notamment dans le design et l'analyse de primitives et protocoles cryptographiques[86]».

Operating systems and security – VUB[87]. Ce cours est enseigné dans la faculté d'ingénierie dans le département d'Électronique et d'Informatique. Ce cours aux compétences techniques poussées permet d'acquérir des connaissances entre autres en : menace de sécurité, «invaders», malicious software, Windows sécurité, etc. La particularité de ce cours est qu'il est donné sous la forme d'un MOOC[88] avec une aide à distance.

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: voir glossaire.

5.3 Les Hautes Écoles

Un bon nombre de Hautes Écoles donnent également des formations en Cybersécurité ou intègrent des cours sur le sujet dans une formation plus générale en informatique (la liste du CCB[89]). Sous la forme de bachelier, de master ou de cours à part entière, ces formations sont de plus en plus nombreuses dans les Hautes Écoles bruxelloises.

5.3.1 Bachelier de spécialisation en sécurité des réseaux et systèmes informatiques - HEB[90]
Cette année de spécialisation se caractérise par un horaire adapté (possibilité d'étaler sur deux ans) et se divise en trois objectifs :
1. Agir de façon autonome et en équipe,
2. S'inscrire dans une démarche sécuritaire suivant une méthode,
3. Mobiliser les savoir-faire spécifiques à la sécurisation d'un système d'information.

Elle permet au détenteur d'un bachelier ou master en informatique d'acquérir des compétences dans le domaine de la Cybersécurité en une année de spécialisation.

5.4 Les certifications et la formation continue

La certification est un bon moyen d'acquérir des compétences spécifiques dans un domaine précis. « *Malheureusement, ces cours, souvent privés, sont payants et à des prix parfois exorbitants* », nous explique Jean-Jacques Quisquater, expert de la cryptographie à l'UCL.

La formation continue est également présente sur le marché de la formation en Cybersécurité. On retrouve une formation continue en Cybersécurité en cours de préparation à l'UCL[91].

5.4.1 La certification en Data Protection Officer
Étant donné l'obligation émanant du GDPR d'engager des DPO, ce genre de formation fleurit sur le marché bruxellois. Nous allons analyser deux d'entre elles.

1. Le certificat en protection des données – DPInstitute[92]
Cette formation est organisée en 5 jours et prépare au poste de Délégué à la Protection des Données (DPO).
Les cours abordent la législation sur le droit à la vie privée en Europe, le travail de DPO, le management des risques et de la vie privée, audit et contrôle, gestion des incidents …

2. Data Privacy security management – ICHEC[93]
Formation de 6 jours qui, comme la précédente, a pour objectif de maitriser les nouvelles obligations du DPO. À l'issue de la formation, l'étudiant doit savoir gérer une communication de crise, identifier le risque en matière de sécurité de l'information, appréhender le rôle et le positionnement stratégique du DPO au sein de l'organisation, etc.

89. https://www.vub.ac.be/en/study/fiches/94249/operating-systems-and-security
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/fr/formations/le-certificat-en-protection-des-donnees/
93. https://www.ichecformationcontinue.be/fr/data-privacy-security-management.html?IDD=553648329&IDC=138

5.5 Des formations de courtes durées

5.5.1 Evoliris

La particularité d'Evoliris est d'offrir un catalogue de formation actualisée de courte durée. Les formations suivantes ont un lien avec la Cybersécurité.

Cyberdéfense et anti-intrusion : cette formation de 5 jours permet de comprendre le fonctionnement des attaques informatiques afin de mener à bien un test d'intrusion et d'élaborer des contre-mesures.

Sécurité d'un poste de travail Windows : couvre les aspects essentiels de la sécurité d'un poste de travail Windows dans des usages de plus en plus mobiles,

Sécurité Linux : sécuriser et auditer un serveur Linux.

Ces formations orientées métier se basent sur la réalité de terrain et les besoins du marché de l'emploi pour permettre aux stagiaires de bénéficier de formations complètes en un laps de temps restreint.

5.5.2 Intec

ICT Security Specialist[94] : destinée aux chercheurs d'emploi maitrisant le néerlandais, cette formation permet d'obtenir des compétences réseaux et serveurs. Elle permet également de connaitre les dernières technologies liées à la sécurité. Les matières enseignées sont : Protection des Périphériques Réseau CISCO, Authentification, Autorisation, Comptabilité, Mettre en Œuvre les Technologies de Pare-Feu CISCO, Systèmes Cryptographiques, Implémenter des VPN CISCO, Sécuriser les Réseaux locaux, Sécurité des Rôles les plus courants de Windows Server (AD, DNS, DHCP, IIS, WSUS, Serveur de fichiers), Exchange, Configuration(s) de Base, Virtualisation, ITIL, Pare-feu.

Digital Skills - Cybersecurity[95] : formation de deux semaines qui permet de développer les compétences numériques en Cybersécurité.

5.6 Autres formations

5.6.1 Cyber WayFinder

Nous avons déjà évoqué cette initiative dans le chapitre : Problème d'image et mixité au cœur du problème. Cette formation adressée aux femmes qui désirent travailler dans les métiers de la Cybersécurité s'articule autour de deux axes[96] : dans un premier temps, des Bootcamps[97] sur la sécurité sont organisés. Ensuite, pendant le reste de la formation, des cours de perfectionnement sont donnés avec notamment des exercices en laboratoire (des cours sur le Risk Management, des cours de cryptographies, des cours sur la mesure GDPR, etc.).

5.6.2 Formation pour entreprises

Cours de sensibilisation ou cours techniques, à destination du management ou des employés; les formations destinées aux entreprises sont une solution pour adopter une culture de la Cybersécurité au sein de l'entreprise. La formation est soit donnée par l'entreprise (généralement, c'est le CISO qui se charge de donner le cours), soit c'est un prestataire externe

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 : voir glossaire

qui s'en charge. Elle se donne dans les locaux de l'entreprise ou via des formations e-learning. Le CCB, en collaboration avec l'IFA, a mis en place des formations à destination des managers et IT qui travaillent au sein d'une autorité publique fédérale[98]. Ces formations de quelques jours sont diverses et peuvent se donner sur le lieu de travail. La Solvay Brussels School propose également une formation de 5 jours « *Programme in European Data Protection* ». Cette formation permet d'obtenir une certification pour le métier de DPO[99].

5.6.3 L'e-learning

L'e-learning reste un bon moyen de se mettre à niveau dans le domaine de l'informatique. Il existe également des formations liées à la Cybersécurité. On peut notamment citer «l'Eurometropolitan E-Campus[100]» avec sa formation en Cybersécurité qui se divise en 5 modules. Cette formation est notamment destinée aux entreprises et aux PME afin de sensibiliser le personnel à la sécurité. L'e-learning est souvent une solution envisagée pour former le personnel aux mesures de sécurité.

98. https://www.ofoifa.belgium.be/fr/cybersecurite-une-offre-de-formation-elargie-tant-pour-les-managers-it-que-pour-les-collaborateurs
99. http://exed.solvay.edu/fr/11-program/221-programme-in-european-data-protection
100. http://www.ee-campus.be/index.php/formations

Conclusion

La Cybersécurité est devenue en quelques années un enjeu européen, fédéral, régional, mais aussi économique et sociétal. Dans l'ensemble, nous avons constaté à l'issue de ce rapport plusieurs problématiques :

1. Bruxelles est encore loin d'être mature pour devenir une ville de la Cybersécurité, mais sa position centrale en Europe lui donne les clés pour se positionner en tant que telle,
2. En Belgique, il y a un écart grandissant entre l'offre de profils-métiers sur le marché de l'emploi et la demande de recrutement,
3. Cet écart est en partie impacté par le manque de formations qualifiantes disponibles en Belgique,
4. Il y a un éternel problème de sensibilisation. La solution serait d'adapter et de renforcer la communication vers les différents publics (enfants, managers d'entreprise, employés, etc.), mais c'est un travail de longue haleine qui doit être constamment répété afin de susciter des réflexes automatiques de sécurité,
5. Un référentiel métier universel est inexistant et les définitions des profils et de leurs compétences sont floues,
6. Il y a souvent un écart entre les formations enseignées et la réalité de terrain,
7. La presse et les services publics peuvent jouer un rôle de transmission des bonnes pratiques,
8. Le problème de recrutement peut également se comprendre à travers le problème de mixité.

Des pistes de solutions et des recommandations

Tout au long de ce rapport, nous avons tenté de mettre en avant les problématiques de la Cybersécurité à travers les différents axes de Bruxelles (économique, politique, académique et au niveau des profils métiers). La situation n'est pas simple entre les problèmes de sensibilisation (comment atteindre les différents types de publics et les sensibiliser à la Cybersécurité ?), le manque de structure au niveau des profils-métiers (titres de fonction trop nombreux et descriptifs de postes trop flous), le manque de maturité de Bruxelles (fragmentation des instances politiques, volonté de centralisation via le CCB, …) et les problèmes liés au recrutement (problème de mixité, manque de diversité des profils, manque de profil sur le marché de l'emploi belge, …).

En conclusion, voici une série de recommandations ou pistes de réflexion en complément du débat sur la Cybersécurité à Bruxelles.

1. Positionner Bruxelles en tant que Capitale européenne de la Cybersécurité

De par sa position stratégique au sein de l'Europe et en accord avec les initiatives de l'Europe, Bruxelles doit montrer l'exemple en appliquant une stratégie de Cybersécurité. Or, à l'heure actuelle, notre capitale souffre d'un manque de maturité face à cette problématique.

Des pistes de réflexion sont proposées :

- Mise en avant des actions des institutions qui œuvrent pour la Cybersécurité, à travers la communication intensive et la centralisation des informations sur des plateformes qui deviendraient des outils de références.
- En termes d'emploi, Bruxelles, de par sa position stratégique, doit attirer les talents et les professionnels des métiers liés à la Cybersécurité.
- Les formations doivent refléter une concertation commune entre les besoins des entreprises et les acteurs de la formation.

2. Commencer la sensibilisation dès le plus jeune âge

La sensibilisation est devenue un enjeu et un défi. Mais jusqu'à quel point peut-on imposer aux gens d'adopter les bonnes mesures de prévention ? La grande difficulté est d'atteindre les individus qui ne se sentent pas concernés par le problème. Nous l'avons vu ; la plupart du temps, le facteur humain est le maillon faible de la sécurité. Sensibiliser les citoyens dès le plus jeune âge par l'école et lors d'activités extrascolaires est une solution. Il existe encore trop peu d'initiatives de ce type en Belgique. Connaitre les possibilités d'attaques permet de mieux se défendre préventivement, ainsi il faut éduquer les enfants dès le plus jeune âge et en continu. Le meilleur moyen d'atteindre les plus jeunes est de prioriser la sensibilisation des parents et des enseignants en premier lieu. Ce sont eux, dans leurs avertissements quotidiens, qui vont distiller les bonnes pratiques. **Des interventions dans les écoles** permettent de transmettre des outils pédagogiques à destination des professeurs et parents qui souhaitent éduquer leurs enfants à la sécurité sur le Net. Il s'agit de mettre entre les mains des adultes des astuces pratiques pour transmettre ce savoir aux plus jeunes afin qu'ils puissent appliquer les notions de base de manière inconsciente. Les initiatives comme ClickSafe de Childfocus[101] doivent se développer pour avoir une meilleure visibilité.

3. Multiplier les moyens de prévention dans les entreprises

La sécurité en entreprise est une problématique récurrente. On doit différencier deux types de cibles : le management et les employés. Tout d'abord, le management est souvent difficile à atteindre. En général, quand la direction est consciente de la sécurité, la politique de sécurité est plus facile à instaurer dans la gestion de l'entreprise. Ensuite, les employés eux aussi ont besoin d'une communication spécifique leur rappelant les règles de base de sécurité. La politique de sécurité doit s'appliquer à tous et peut se manifester à travers plusieurs recommandations répétées. Pour atteindre l'employé, il faut parvenir à l'impliquer dans la sécurité de la société. En général, c'est le rôle du DPO et du CISO de communiquer sur les mesures de sécurité.

Chaque entreprise devrait mettre en place une **politique de sécurité** valable pour tous les membres de l'entreprise. Cette sensibilisation est généralement prise en charge par le responsable de la sécurité qui se donne pour mission de graver dans l'esprit de ses collègues une culture de la sécurité. Ce responsable doit être épaulé par la direction de son entreprise qui doit donner l'exemple. Aucun moyen ne doit être épargné pour sensibiliser : affichettes sur les murs et même jusque dans les toilettes (histoire vraie !), mailing de rappel de sécurité, ajout d'une Cyber Security Policy dans le règlement de travail, tests réguliers des infrastructures, organisation de conférences et de formations chaque année pour rappeler les usages. Il faut faire comprendre que l'employé est responsable de ses actes qui peuvent avoir un impact sur la sécurité des infrastructures de l'entreprise. Il faut également faire comprendre que la sécurité n'est pas qu'une question d'informatique, cela peut se manifester aussi par une intrusion physique dans l'entreprise (Social engineering[102]).

En ce qui concerne **les petites structures du type PME ou TPE** pour lesquelles il n'est pas réaliste d'engager un expert de la Cybersécurité à temps plein, il existe deux solutions :

- Engager un informaticien ayant des compétences générales qui pourrait (à la suite d'une courte formation) consacrer du temps à la sécurité.
- Faire appel à des agences de consultance spécialisées dans la sécurité (notons qu'avec le boom des besoins du marché de la sécurité, il y a une explosion de la création de ces types d'agences).

101. http://www.childfocus.be/fr/prevention/clicksafe-tout-sur-la-securite-en-ligne
102. Social engineering : voir glossaire

4. Aides financières et ressources administratives pour conseiller les entreprises

Comment mettre au point des bonnes pratiques de gouvernance informatique à l'échelle d'une PME ou TPE ? À Bruxelles, il n'existe aucune aide financière concrète facilitant le passage des entreprises à la prise en compte de la sécurité. En Région Wallonne, il existe des aides et déductions fiscales pour les PME qui investissent dans des solutions numériques. Peu de personnes en connaissent l'existence. Il faudrait donc les mettre en évidence et communiquer le cadre et les détails de ce type de mesures. Ces « chèques Cybersécurité » accordés aux entreprises se divisent en deux catégories : le chèque Audit (définition d'une politique de sécurité *privacy by design*) et le chèque Labellisation coaching (évaluation en vue d'obtenir un label qualité)[103]. Ces initiatives sont issues du constat que les PME sont conscientes des problèmes de Cybersécurité (on l'a vu dans le chapitre dédié aux PME), mais n'ont pas les moyens de mettre en place une stratégie de Cybersécurité. Ces mesures sont très intéressantes et la Région de Bruxelles-Capitale devrait y réfléchir pour aider les entreprises.

Communiquons également sur les ressources et institutions qui accompagnent et conseillent sur la création d'entreprise ou l'amélioration d'une entreprise. On a déjà mentionné dans le rapport la plateforme 1819[104] et l'incubateur d'entreprises Impulse.Brussels[105].

5. Le secteur public a un rôle à jouer

La Cybersécurité est principalement associée au niveau fédéral même si la régionalisation des activités est de plus en plus présente. Ainsi, la Région de Bruxelles-Capitale et ses services publics ont un rôle à jouer non seulement dans l'accompagnement et le conseil, mais aussi dans la sensibilisation. En effet, les médias qui partagent les actualités de la cybercriminalité mettent le doigt sur le fait que ces menaces sont principalement ciblées sur les institutions publiques. Or, ce n'est pas uniquement le cas. Tout le monde est concerné ! Ainsi, le secteur public doit être transparent et donner l'exemple ; montrer que tout le monde peut être la cible. Car ce n'est pas parce que nous considérons que nous n'avons pas de données sensibles que nous n'intéressons pas les hackeurs. Dans le cas de la sensibilisation, la première étape est de centraliser les informations sur des sites de références à destination de tous les publics et d'en faire la promotion afin que les cibles concernées aient le réflexe d'aller consulter ces sites régulièrement.

6. Résoudre le problème de l'écart entre disponibilité des profils sur le marché et des offres de recrutement

Plusieurs critères entrent en compte. Premièrement, depuis quelques mois, en raison de l'impact des mesures européennes, de nouvelles formations voient le jour pour tout public. Malgré tout, le paysage des formations en Cybersécurité a peu de visibilité. Ensuite, en Belgique, les profils-métiers n'ont pas de référentiels clairs et souffrent d'une mauvaise image. Enfin, les méthodes de recrutement doivent évoluer. L'expérience professionnelle ne doit plus être le critère principal de recrutement. Comme nous l'avons vu dans le chapitre sur les métiers, une étude a constaté que les profils atypiques sont aussi de bons profils. De même, les *softs skills* ont beaucoup d'importance dans les profils liés à la Cybersécurité. La première étape devrait donc être de définir un référentiel universel clair par les acteurs de la formation et de l'emploi afin de faciliter une adéquation entre les besoins des entreprises et les compétences à acquérir. Ensuite, le paysage académique doit se développer et proposer des formations pour tous types de profils (formations longues, formations courtes et qualifiantes, etc.). L'analyse de la problématique nous a permis de découvrir que les formations doivent développer des experts de la sécurité ayant la vocation en eux et pas

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

uniquement les compétences techniques. Les formations doivent inclure cet élément dans leurs offres de cours afin de s'adapter à la réalité de terrain.

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

Le Pôle Formation Emploi ICT ouvrira ses portes à la fin de l'année 2018. Il aura un rôle à jouer dans le contexte de la promotion, la communication et de la formation de la Cybersécurité dans :

- L'offre des formations en Cybersécurité de courtes durées destinées aux chercheurs d'emploi, aux employés, aux enseignants et formateurs et aux étudiants. Ces formations prendront la forme de formation technique et informatique, mais également juridique (exemples : formation GDPR, formation soft skills …).

- L'offre de formation qualifiante longue et/ou de spécialisation pour les chercheurs d'emploi.

- La transmission d'un message à travers la participation et l'organisation d'événements (conférence, hackhatons[106], association à d'autres institutions lors d'événements divers et variés).

- La promotion des métiers et la sensibilisation sont des axes importants dans la constitution du Pôle. Comme nous l'avons précédemment développé dans le rapport, il y a encore un important travail de sensibilisation à faire auprès des plus jeunes à travers les professeurs et les parents. Le Pôle pourra fournir des conseils afin de fournir aux adultes des outils pédagogiques permettant de sensibiliser les plus jeunes.

106. Hackhatons : voir glossaire

Remerciements

Pour la rédaction de ce rapport, nous avons fait appel à des experts du domaine qui ont bien voulu partager leurs connaissances et leur savoir-faire sur la Cybersécurité. Nous les remercions pour le temps et l'attention qu'ils nous ont consacrés.

Jean-Marc André - UNIWAN

Olivier Bogaert - FCCU

Andries Bomans – CCB

Ferdinand Casier - AGORIA

Thierry Cools - Bruxelles formation

Marc Daem – CIRB

Vincent Defrenne - NVISO

Florianne de Kherchove – AGORIA

Tanguy De Lestré – Cabinet de la Secrétaire d'État à la Région Bruxelles-Capitale Bianca Debaets

Benoit Fosty – CIRB

Jeroen Franssen – AGORIA

François Goffinet – Sinibaldi

Nicolas Harmel - Cabinet du ministre Didier Gosuin, ministre de l'Économie et de l'Emploi de Bruxelles

Jean-Jacques Quisquater – UCL

Gregorio Matias – MCG

Philip Richardson – Bruxelles formation

Benoit Rousseaux – Digital Security

Bruno Schröder - Microsoft, MIC

Valery Vander Geeten – CCB

Pascal Van de Walle - CIRB

Nicolas Vautrin – INNOVIRIS

Glossaire

Bitcoin : Une monnaie cryptographique et un système de paiement pair-à-pair. Source - Wikipedia.

Compliance : Conformité.

Cyber-résilience : Capacité à se préparer et s'adapter à des conditions en perpétuelle évolution ainsi qu'à récupérer rapidement ses capacités suite à des attaques délibérées, des accidents, des catastrophes naturelles ou encore des incidents dans le cadre de l'utilisation de moyens informatiques et de communication. Source définition : http://www.ab-consulting.fr/blog/non-classe/cyber-securite-vs-cyber-resilience

Encryptage : procédé de cryptographie qui consiste à rendre illisibles des données pour les personnes qui ne possèdent pas la clé d'accès.

Forensique : L'analyse forensique en informatique signifie l'analyse d'un système informatique après incident. Source : Wikipedia.

Hackathon : désigne un événement où un groupe de développeurs volontaires se réunissent pour faire de la programmation informatique collaborative, sur plusieurs jours. C'est un processus créatif fréquemment utilisé dans le domaine de l'innovation numérique. Source : Wikipedia

Hacking : ou piratage informatique. Ensemble de techniques permettant d'exploiter les failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.

Malware : un logiciel malveillant ou maliciel est un programme qui infecte un système informatique.

MOOC: Massive Open Online Course. Le MOOC est un cours ouvert et massif en ligne que l'on peut associer à une formation ouverte à distance.

NotPetya: Ransomware du même type que Wannacry.

Phishing Ou hameçonnage : Une technique de fraude qui consiste à obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Source : Wikipédia.

Pop-Up : Parfois appelée « fenêtre intruse » ou « fenêtre surgissante », est une fenêtre secondaire qui s'affiche, sans avoir été sollicitée par l'utilisateur (fenêtre intruse), devant la fenêtre de navigation principale lorsqu'on navigue sur Internet. Source : Wikipedia.

Privacy by design : Il s'agit d'intégrer la protection des données dès la conception et le fonctionnement du système ou du réseau informatique, mais également de pourvoir à l'élaboration des pratiques responsables.

Ransomware (rançongiciel) : logiciel malveillant qui prend en otage des données personnelles. La victime est sommée de payer une rançon pour récupérer l'utilisation de ses données.

Social engineering : ou ingénierie sociale. Cette technique fait référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Les escrocs exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.). Source : Wikipédia.

Wannacry: Ransomware qui exploite une faille de Microsoft Windows. Ce ransomware s'est sans doute diffusé par une campagne de mailing massif. Une fois le virus installé et les fichiers encryptés, le virus demande une rançon en bitcoin.

White paper: ou livre blanc. Recueil d'informations objectives et factuelles destiné à un public déterminé pour l'amener à prendre une décision sur un sujet particulier. Source : Wikipédia.

Institutions citées

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

CEIS : Conseil Européen d'Intelligence Stratégique https://ceis.eu/fr/accueil/

CIRB : Centre d'Informatique pour la Région Bruxelloise http://cirb.brussels/

BELNET : réseau de recherche national belge qui fournit notamment une connexion Internet haut débit et des services associés aux universités, aux hautes écoles, aux centres de recherches et au gouvernement. https://www.belnet.be/fr

FCCU: Federal computer crime unit. https://www.police.be/5998/fr/a-propos/directions-centrales/federal-computer-crime-unit

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

OCDE : Organisation de Coopération et de Développement Économiques. http://www.oecd.org/fr/

PFE : Pôle Formation Emploi ICT

RÉDACTEUR
Christina Galouzis

POST-ÉDITEUR
Luc Huygh

ÉDITEUR RESPONSABLE
Jean-Pierre Rucci

CONCEPTION GRAPHIQUE
www.sergeantpaper.be

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

CONTACT
Evoliris Asbl
Rue de la Borne,14 A I 1080 Bruxelles I 02/475 20 00
info@evoliris.be I www.evoliris.be

Evoliris

EVOLIRIS asbl est le Centre de Référence Professionnelle bruxellois dans le domaine des Technologies de l'Information et de la Communication (TIC). Dès sa création, en 2006, le centre s'est donné pour mission de sensibiliser, informer et former aux métiers TIC. EVOLIRIS agit prioritairement auprès de trois groupes cibles : **les élèves et les enseignants** dans le cadre notamment de campagnes de sensibilisation aux métiers, **les demandeurs d'emploi** grâce à notre offre de formations et à notre aide en matière de guidance de recherche d'emploi. Et enfin, **tous les travailleurs,** en particulier les employés du secteur qui, grâce à nos formations, peuvent évoluer dans leur domaine professionnel.

Pour plus de renseignements : **www.evoliris.be**

Contact :

Rue de la borne, 14 - Bâtiment A I 1080 Bruxelles I 02 475 20 00 I info@evoliris.be