LE CLUSTER OPEN VOUS PRESENTE

NAISSANCE D'UNE FILIÈRE D'AVENIR EN NC

TOUR D'HORIZON ET PERSPECTIVES

contact@open.nc
73.11.60
www.open.nc

Juillet 2020
Par Xavier BAHUON et
Laurent RIVATON

Introduction

Cet OPEN BOOK fait suite à l'OPEN MEETING du 23 juillet 2020 qui s'est tenu à la CCI. Nous avons retranscrit par écrit la conférence donnée ce soir-là.

Jean-Marc Brecard (Codigis) était un charge de l'animation.
Xavier Bahuon (Cyber Action), diplômé d'un Master en cybersécurité, certifié CISSP et formateur agréé DFPC, a rédigé les parties 1 et 2.
Laurent Rivaton (AdDo), certifié CEH, CISSP, OSCP, et formateur agréé DFPC a traité les parties 3 et 4.

Lors de cette soirée, les invités avaient la possibilité d'interagir avec les intervenants via l'application Sli.Do et ainsi poser des questions et réagir aux commentaires. L'ensemble des questions posées et leurs réponses font l'objet de la dernière partie de ce document.

En espérant que cette restitution saura vous convaincre du potentiel de la filière cybersécurité en Nouvelle-Calédonie.

Bonne lecture.

SOMMAIRE

1ere PARTIE

LES GRANDS PRINCIPES

QU'EST-CE QUE LA CYBESÉCURITÉ ?

La cybersécurité se définit comme la protection des systèmes d'information, comprenant en grande partie l'informatique.

Pour aborder les trois principaux besoins de la cybersécurité (la disponibilité, l'intégrité et la confidentialité), nous allons associer le système d'information à une voiture.
La voiture et le système d'information fonctionnent avec :

- de l'énergie (essence ou électricité),
- un moteur (implanté sous le capot ou dans un boitier d'ordinateur),
- des commandes (sous la forme d'un tableau de bord, d'un volant et des pédales ou avec l'ensemble écran, clavier et souris)
- des données (assimilable aux roues de la voiture qui la font avancer et qui tracent la route).

LA DISPONIBILITÉ

La disponibilité est la propriété d'être accessible et utilisable par une entité autorisée.
Si nous continuons notre parallèle avec la voiture, le chauffeur qui possède la bonne clé de contact est l'entité autorisée, mais ce n'est pas forcément suffisant pour l'utiliser… En effet, lorsque vous tournez la clé de contact et que la voiture ne démarre pas, c'est un problème de disponibilité.
Lorsque l'on souhaite démarrer son système d'information, la résolution peut être :

- Facile, une prise à rebrancher pour un ordinateur ou une batterie à recharger pour la voiture.
- Difficile, le remplacement d'un disque dur ou d'une autre pièce pour l'ordinateur ou un démarreur ou une partie du moteur à changer pour la voiture.

Les problèmes de disponibilité peuvent se produire à tout moment. Le coup de la panne d'essence en est un exemple parce qu'il n'y a pas eu l'application de certaines règles. La voiture doit être régulièrement entretenue pour vérifier le réservoir d'essence, mais aussi l'huile, le liquide de refroidissement, la pression des pneus, la révision… Dans le numérique, l'hygiène informatique doit également être régulièrement appliquée. Celle-ci comprend les mises à jour des logiciels, la mise en place de pare-feu, l'installation d'antivirus, la planification de sauvegardes régulières, le choix de bon mot de passe… A minima, toutes ces règles sont nécessaires pour une bonne continuité des activités.

L'INTÉGRITÉ

Il ne suffit pas que la voiture ou le système d'information soient suffisamment sûrs, il faut également que le conducteur, que l'humain ait un minimum de maitrise des outils à sa disposition.

Prenons le cas de l'intégrité qui est la propriété de protection de l'exactitude et de l'exhaustivité des actifs. En voiture, nous donnons des ordres de direction avec le volant et la voiture obéit avec une intégrité quasi parfaite… Dans certaines circonstances particulières, et encore plus rarement lorsque l'on est prudent, la voiture peut tourner dans le sens opposé à la direction qui lui a été ordonnée. C'est le cas, lorsque la route est mouillée ou lorsque le conducteur doit réagir en situation d'urgence pour un évitement sur la route.

En cyber, lorsque vous payez un fournisseur en ligne, le copier/coller que vous effectuez entre le numéro de compte du fournisseur et le site de votre banque obéit à une intégrité quasi parfaite… Dans certaines circonstances particulières, et encore plus rarement lorsque l'on a fait une vérification, le numéro de compte peut avoir été modifié par un autre, suivant des méthodes d'attaques diverses et variées.

Dans tous ces cas et sans être obligatoirement un expert en informatique ou un pilote de formule 1, un humain qui a son permis de conduire ou qui a suivi une sensibilisation en cybersécurité sait, très souvent, comment agir correctement et rapidement.

LA CONFIDENTIALITÉ

La confidentialité est la propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés.
En voiture, le numéro de la plaque d'immatriculation vous garantit une certaine confidentialité. Celle-ci est rendue obligatoire par la loi pour ne pas être obligé d'indiquer à l'extérieur de la voiture, l'état civil du propriétaire du véhicule.

En informatique, la loi sur le RGPD protège les données personnelles des utilisateurs pour que celles-ci ne soient pas diffusées aux quatre coins de la planète, sans aucune maitrise de l'utilisateur.
Plus concrètement, lorsque nous entreposons des objets dans notre voiture, nous les disposons rarement dans l'habitacle parce qu'ils seraient à la vue de n'importe quelle personne. Par contre, le coffre du véhicule qui ferme à clé permet d'obtenir une confidentialité qui est bien appréciable.
En informatique, nous pouvons communiquer ou travailler avec plus ou moins de confidentialité. Il faut en tenir compte suivant l'importance des données qui seront concernées.

2e PARTIE

ÉTAT DES LIEUX

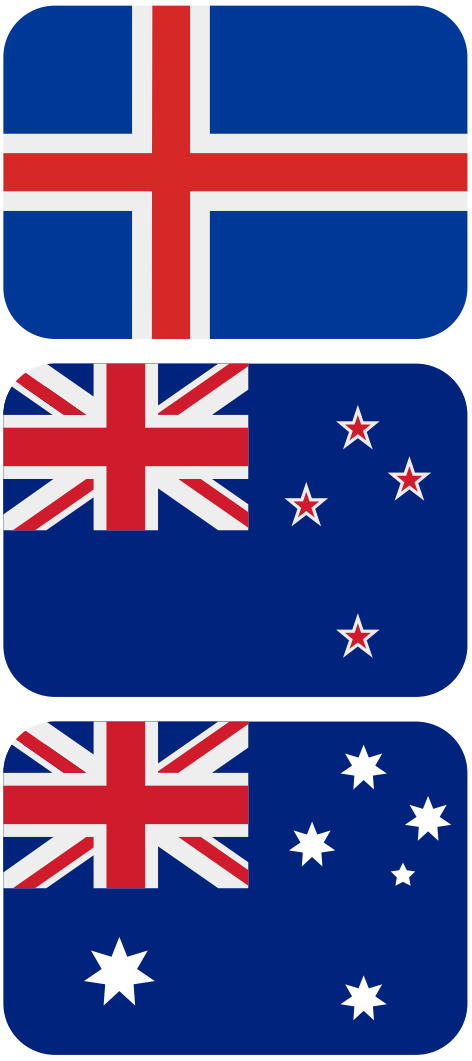
L'INDICE D'EXPOSITION AU CYBER-RISQUES

De ces grands enjeux de la cybersécurité découlent des risques. La science de la cybersécurité étant relativement jeune, les indicateurs de la cybersécurité en Nouvelle-Calédonie sont encore rares. Nous nous sommes donc intéressés à certains indices que nous avons essayé de transposer à la Nouvelle-Calédonie.

L'indice d'exposition aux cyber-risques (CRI) mesure le risque d'être victime de cybercriminalité selon le pays de résidence, sur une échelle de 0 à 1. Plus l'indice est élevé et plus le risque de cybercriminalité est élevé.

L'INDICE D'EXPOSITION AU CYBER-RISQUES

Une étude a déjà été réalisée en 2020 par Statista. D'après cette étude, l'Islande, qui est une île comparable à la Nouvelle-Calédonie est le pays le plus exposé aux risques cyber dans le monde. Nos proches voisins, comme la Nouvelle-Zélande ou l'Australie sont classées respectivement à la 8éme et à la 16éme place des pays les plus exposés aux risques cyber.



Toujours d'après cette étude, les indicateurs qui sont des facteurs aggravants dans le calcul du CRI sont :

- Les pays développés avec des revenus élevés.
- Les pays avec un taux d'utilisation des outils numériques importants.

SOURCE : STATISTA

LES INDICATEURS DU CRI

La Nouvelle-Calédonie n'a pas été étudiée dans cette étude.
Nous avons donc repris les 14 indicateurs permettant d'élaborer le calcul de l'indice CRI. Parmi ceux-ci, nous n'avons pu récolter des données que pour 8 d'entre eux. Ces derniers sont tout de même bien répartis entre les indicateurs sociaux et techniques et surtout nous avons les indicateurs qui ont le plus d'influence dans le calcul du CRI.

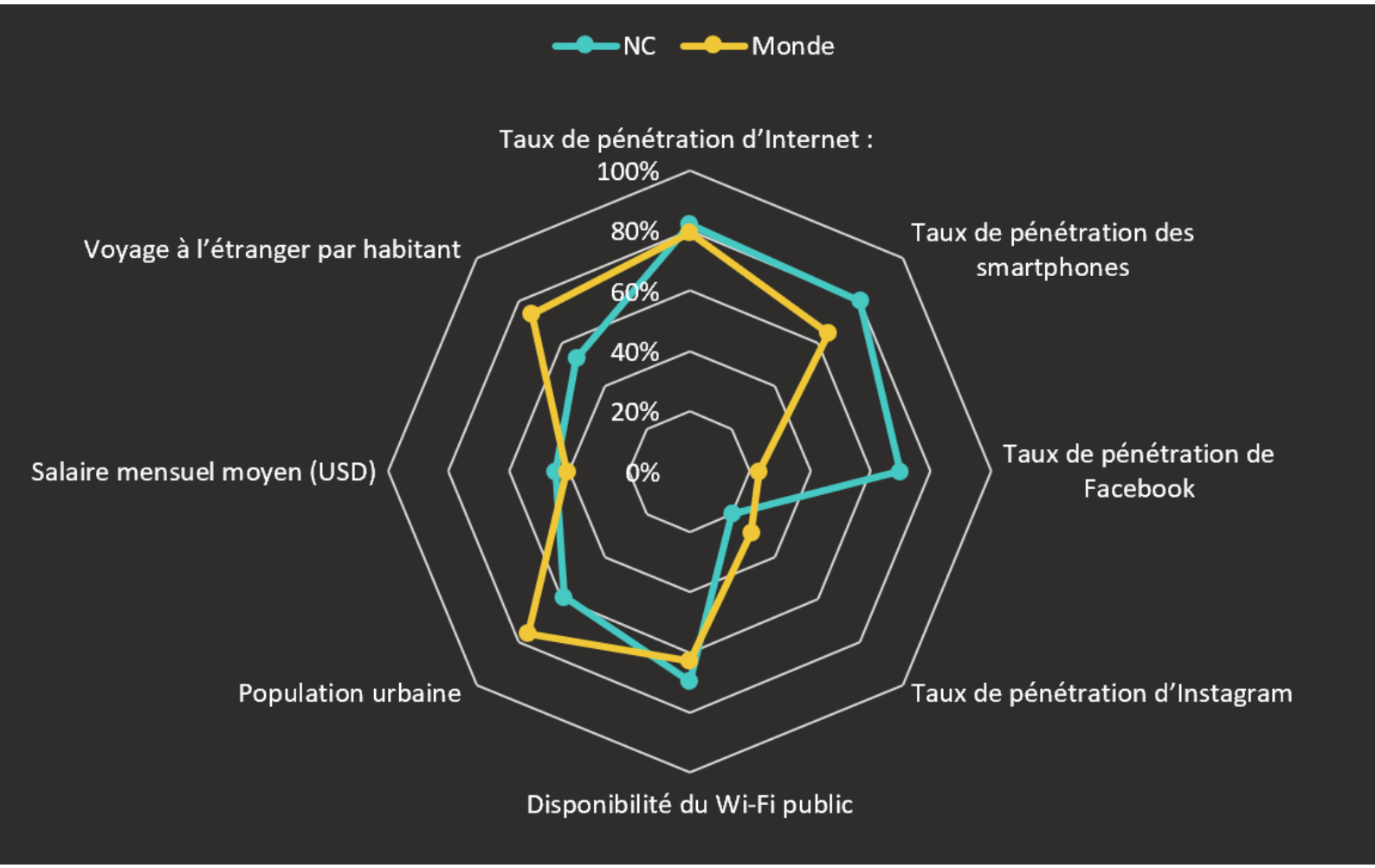
À noter que l'indice mondial de cybersécurité (faisant partie des 14 indicateurs du CRI) n'a pas été calculé pour la Nouvelle-Calédonie. L'indice mondial de la cybersécurité est un indice lié à la géopolitique de la cybersécurité. À la différence, l'indice CRI est lié à la cybercriminalité. De ces 2 indices, le CRI est donc le facteur de risques le plus représentatif pour les entreprises.

Les données récoltés des indicateurs pour la Nouvelle Calédonie

- **Population urbaine : 59%**
- **Salaire mensuel moyen : 2 844,23 $**
- **Voyage à l'étranger : 0,53 par an/habitant**
- **Taux de pénétration d'Internet : 82%**
- **Taux de pénétration des smartphones : 80%**
- **Temps passé sur Internet**
- **Taux de pénétration du commerce électronique**
- **Taux de pénétration des jeux en ligne**
- **Taux de pénétration de la VoD**
- **Disponibilité du réseau Wi-Fi public / 3,0 pour 100 hab**
- **Taux de pénétration de Facebook : 70%**
- **Taux de pénétration d'Instagram : 20%**
- **Indice de criminalité**
- **Indice mondial de cybersécurité**

SOURCE : ONNC - BAROMÈTRE NUMÉRIQUE 2018 / ETUDE HOOTSUITE WE ARE SOCIAL 2019

POSITION DE LA NOUVELLE-CALÉDONIE



Lorsque l'on compare ces 8 indicateurs entre les données de la Nouvelle-Calédonie et la moyenne mondiale, on remarque que ceux-ci sont plutôt dans la moyenne mondiale, en particulier pour le salaire mensuel moyen ou bien au-dessus de la moyenne mondiale pour le taux d'utilisation des outils.

SOURCE : ONNC - BAROMÈTRE NUMÉRIQUE 2018 / ETUDE HOOTSUITE WE ARE SOCIAL 2019

CLASSEMENT DES 50 PAYS SELON L'INDICE D'EXPOSITION AUX CYBER-RISQUES

Rang	Pays	CRI
1	Islande	0.839
2	Suède	0.809
3	Émirats Arabes Unis	0.774
4	Norvège	0.729
5	États-Unis	0.713
6	Singapour	0.670
7	Irlande	0.664
8	Nouvelle-Zélande	0.660
9	Denemark	0.657
10	Royaume-Uni	0.647
11	Israël	0.646
12	Finlande	0.641
13-15	Belgique	0.621
13-15	Canada	0.621
13-15	Chili	0.621
16	Australie	0.620
17	Pays-Bas	0.617
18	Argentine	0.601
19	Suisse	0.597
20	Corée du Sud	0.556
21	Allemagne	0.530
22	Brésil	0.519
23	Autriche	0.503
24	Italie	0.500
25-26	Arabie Saoudite	0.484
25-26	Espagne	0.484
27	Grèce	0.481
28	Malaisie	0.479
29	République tchèque	0.474
30	France	0.467
31	Estonie	0.456
32	Portugal	0.454
33	Mexique	0.450
34	Lituanie	0.447
35	Japon	0.444
36	Hongrie	0.441
37	Lettonie	0.429
38	Turquie	0.386
39	Pologne	0.367
40	Russie	0.364
41	Ukraine	0.361
42	Iran	0.349
43	Philippines	0.337
44	Thaïlande	0.334
45	Chine	0.326
46	Afrique du Sud	0.300
47	Indonésie	0.291
48	Irak	0.290
49	Nigeria	0.239
50	Inde	0.186

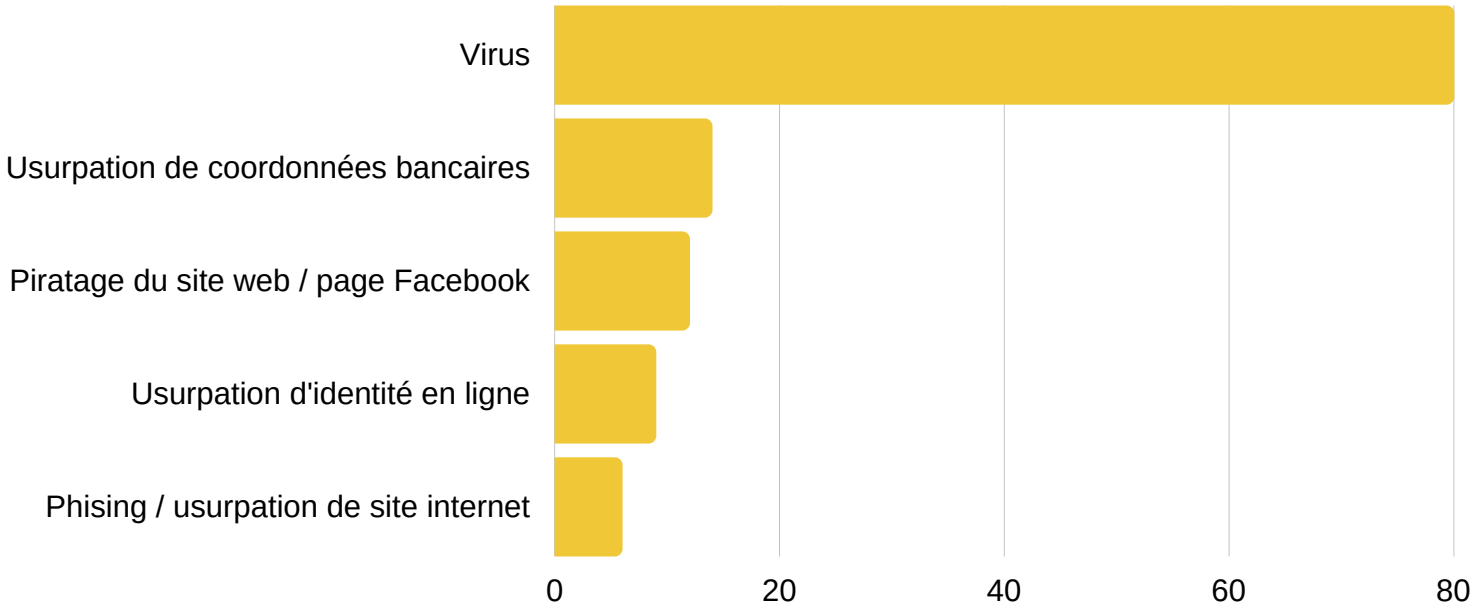
D'après nos calculs, la tendance de la Nouvelle-Calédonie se situerait entre la 15éme et 20éme place dans le classement ci-dessus.
La Nouvelle-Calédonie serait donc plus à risque que des pays comme la France, le Japon ou même l'Allemagne…

SOURCE : STATISTA

QUELQUES CHIFFRES LOCAUX

Un autre indicateur des cyber-risques en Nouvelle-Calédonie est celui fourni par l'Observatoire du Numérique. 25% est le taux d'entreprises qui ont déjà été victimes d'une attaque au cours de l'année.

25%



Parmi ces victimes, ce sont des virus sont en grande majorité (80%) à l'origine de l'attaque. La deuxième cause d'attaque est l'usurpation de coordonnées bancaires.

SOURCE : ONNC - BAROMÈTRE NUMÉRIQUE 2018

QUELQUES CHIFFRES LOCAUX

La Nouvelle-Calédonie est clairement exposée aux cyber-risques. Est-ce que l'on fait le nécessaire pour se protéger correctement ?
Précédemment, nous avons évoqué l'hygiène informatique comme une base que toutes les entreprises devraient appliquer.

Pour rappel, cette base doit comprendre à minima tous les points suivants :

- Mises à jour des logiciels et des différents équipements
- Sauvegardes régulières et vérifiées
- Utilisation de bons mots de passe ou d'authentification forte
- Fonctionnement correct d'un antivirus
- Installation et configuration d'un pare-feu (firewall)

À propos de ce dernier point, l'Observatoire du Numérique donne un autre indicateur sur le taux d'utilisation d'un pare-feu dans les entreprises qui n'est que de 13%. C'est un peu comme si 87% de la population en Nouvelle-Calédonie ne mettaient pas de ceinture de sécurité dans sa voiture, non pas par oubli, mais parce qu'il n'y aurait tout simplement pas de ceinture de sécurité dans leur voiture.

SOURCE : ONNC - BAROMÈTRE NUMÉRIQUE 2018

3e PARTIE

CRÉATION DE LA FILIÈRE : COMMENT ET POURQUOI

POURQUOI LA CRÉATION D'UNE FILIÈRE ?

A la question : pourquoi faut-il créer une filière cybersécurité en Nouvelle-Calédonie, la réponse est simplement 13 !
13, c'est le pourcentage d'entreprises équipées de pare-feu sur le territoire d'après le baromètre numérique 2018 publié par l'Observatoire du Numérique de Nouvelle-Calédonie.
Et comme ça a été indiqué dans la première partie de la conférence, si les bonnes pratiques étaient respectées, le pourcentage d'entreprises connectées utilisant un pare-feu devrait être 100 %. Une telle exigence peut sembler excessive mais ce type d'équipement fait partie des protections de base.
Est-ce qu'un constructeur automobile se poserait la question de savoir s'il lui faut des freins ou des ceintures de sécurité dans son nouveau modèle de véhicule ? Non bien entendu. Il en est de même pour un système d'information : la question de mettre en place les protections de base ne doit pas se poser.

Avec 87% des entreprises calédoniennes qui ne mettent pas en place les protections de bases en matière de cybersécurité, il y a à l'évidence un marché local et un réel besoin en matière d'amélioration du niveau de sécurité. C'est pourquoi nous avons décidé de lancer ce projet de création, d'organisation et surtout de développement de toute une filière.

SOURCE : ONNC - BAROMÈTRE NUMÉRIQUE 2018

COMMENT METTRE EN PLACE LA FILIÈRE ?

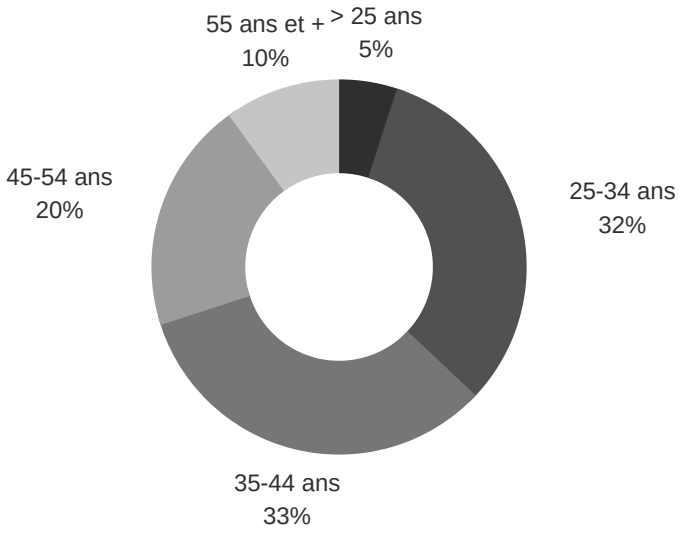
3 axes ont été identifiés pour la mise en place de la filière :

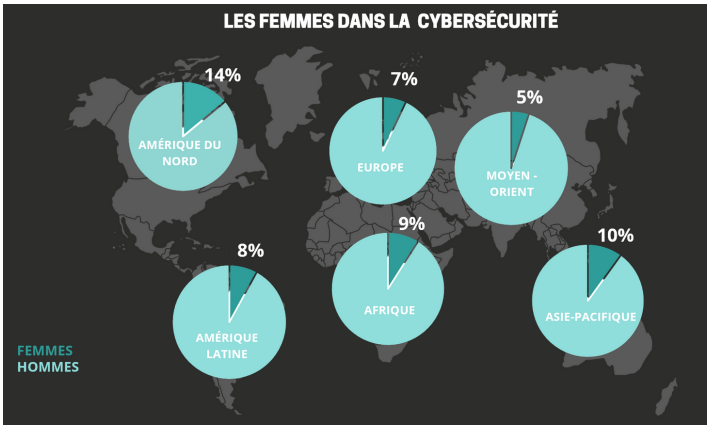
- Le premier axe concerne les futurs professionnels calédoniens de la cybersécurité qui doivent être identifiés : nous devons susciter des vocations.
- Le second axe va porter sur leur formation.
- Le troisième axe a pour objectif de stimuler la demande des entreprises, organisations, etc. de les inciter à entamer une démarche d'amélioration de leur sécurité.

AXE 1 : SUCITER DES VOCATIONS

Notre premier axe : susciter des vocations, détecter des talents. Ce point est évidemment capital : sans professionnels qualifiés il est difficile d'envisager une amélioration de la situation actuelle.
Malheureusement nous sommes aujourd'hui confrontés à un problème d'attractivité des métiers de la cybersécurité. Les métiers du numérique sont généralement mal connus, en particulier leur diversité et cette méconnaissance est encore pire pour les métiers de la cybersécurité.

Ainsi, si on regarde le profil type d'un professionnel de la cybersécurité il y a peu de jeunes.
Avec seulement 5 % qui ont moins de 25 ans contre presque 1/3 de plus de 45 ans.





A noter également qu'il y a peu de femmes. D'évidence nous avons un effort particulier à faire pour toucher un plus large public et probablement remettre en cause un certain nombre de préjugés autour de ces professions.

SOURCES : (ISC)² CYBERSECURITY WORKFORCE, 2019 / 2017 GLOBAL INFORMATION SECURITY WORKFORCE STUDY

AXE 1 : SUCITER DES VOCATIONS

En réalité, il n'y a aucune raison que le profil type ne soit pas représentatif de la population. Il y a d'ailleurs un vrai besoin de diversité et dans certaines spécialités, on pêche toujours par manque d'imagination.
Il est donc capital de constituer des équipes très hétérogènes en termes d'âge, de genre, de culture, etc. dans lesquelles chacun pourra apporter un point de vue original.
A ce sujet, des travaux sont en cours au sein d'OPEN et au-delà des actions de sensibilisations qui vont être amplifiées, un certain nombre de réflexions et d'expérimentations sont en cours pour attirer l'attention sur ces métiers, avec 2 cibles :

- la cible des jeunes avec notamment des travaux avec la MIJ,
- mais aussi un public de professionnels qui voudraient se reconvertir.

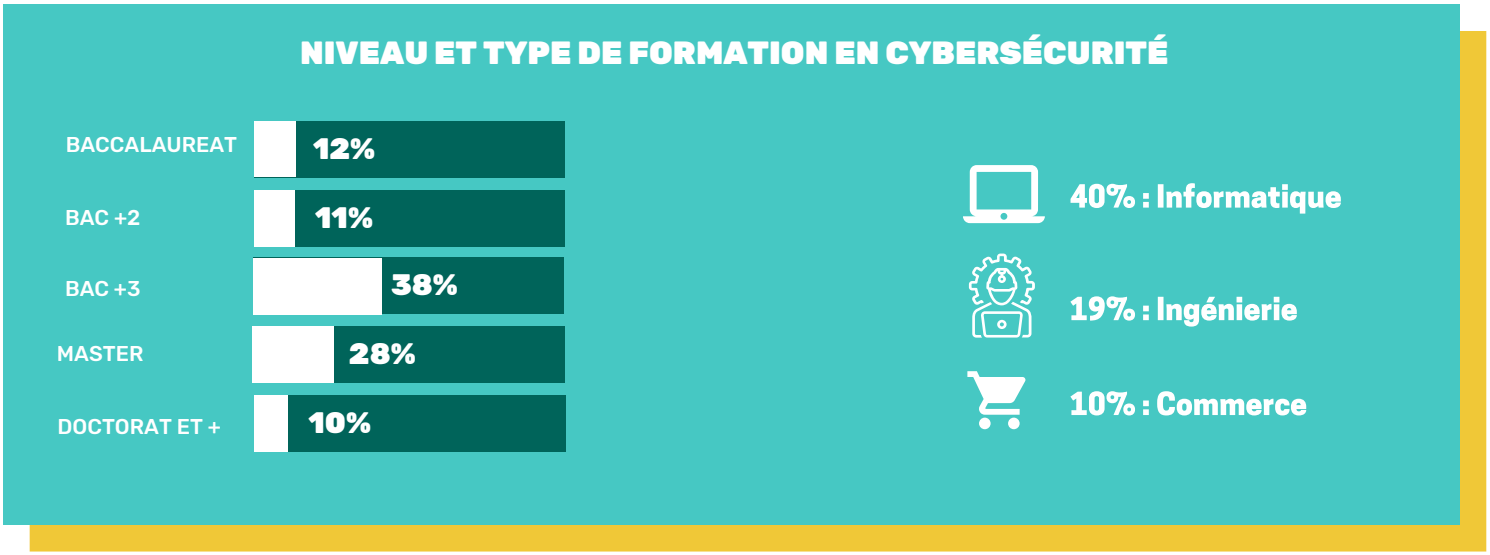
Cette dernière cible (les adultes en reconversion) n'était pas prioritaire jusqu'à présent, mais le contexte actuel de crise sanitaire avec ses impacts économiques qui entrainera probablement de la casse du côté emploi, nous avons estimé qu'il y avait là une opportunité pour proposer à certains des parcours de reconversion vers ces métiers. Dans tous les cas, nos principaux critères de détection sont l'envie et la motivation.

AXE 2 : FORMER

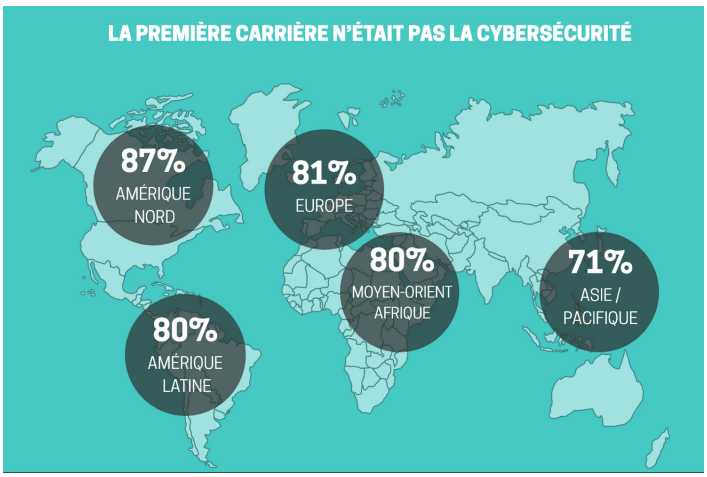
Le volet détection des talents s'adresse à une cible large, sans prérequis en termes de formation initiale. Un dispositif d'évaluation de compétences et de connaissances permettra de déterminer le type de remise à niveau nécessaire avant d'entamer la formation à la cybersécurité proprement dite.

Au sujet du niveau de formation nécessaire, il est important de préciser que contrairement à une idée largement répandue, les métiers de la cybersécurité ne sont pas exclusivement réservés à des personnes ayant un haut niveau de formation.

En effet, si on regarde de nouveau le profil type d'un professionnel de la cybersécurité aujourd'hui, on voit que presque les 2/3 ont un niveau bac, bac+2 ou bac+3.
De plus, seulement 40 % de ces professionnels ont une formation initiale dans l'informatique.



On note enfin qu'environ 80% des professionnels de la cybersécurité actuels n'ont pas commencé leur carrière dans ce secteur. Nous sommes donc très loin du cliché des petits génies de l'informatique, passionnés depuis leur plus jeune âge et ayant fait de très longues études supérieures avant d'arriver sur le marché de l'emploi !



SOURCE : (ISC)² CYBERSECURITY WORKFORCE, 2019

AXE 2 : FORMER

Il y a une grande diversité de métiers dans la cybersécurité. Pour vous donner une idée de cette diversité, voici plusieurs façons de classer ces métiers :

- Défensif / Offensif
- Management / Technique / Juridique
- Architectes / Intégrateurs / Exploitants / Auditeurs

DÉFENSIF / OFFENSIF

En simplifiant à l'extrême, les métiers du défensif se consacrent à la prévention, avec des expertises pour mettre en place des systèmes techniques, des organisations, etc. Le principe est de connaître parfaitement un sujet et que les mises en œuvre soient réalisées dans les règles de l'art. Dans le cas du pare-feu cité précédemment, même le meilleur pare-feu du moment sera totalement inefficace s'il n'est pas correctement configuré. Dans ce cas l'expertise va consister à mettre en oeuvre ce pare-feu en accord avec vos besoins et vos contraintes.
Les métiers de l'offensif se consacrent plutôt à la mise à l'épreuve des systèmes et à la recherche de leurs points faibles. L'expertise va consister à connaitre des technologies, hors considération de marques ou de type d'équipement, et à être très créatif pour contourner les protections mises en place ou trouver des failles de conception, de configuration, etc.

MANAGEMENT / TECHNIQUE / JURIDIQUE

Toujours en simplifiant, les métiers du management sont ceux de la gestion des risques et de la sécurité. Par exemple, le métier de DSI fait partie de cette catégorie.
Les métiers techniques sont ceux qui entourent les outils technologiques comme les administrateurs de bases de données.
Les métiers juridiques enfin sont ceux qui se chargent de la conformité réglementaire. Le RGPD est un exemple de contrainte règlementaire ayant un fort impact sur la sécurité des systèmes d'information.

AXE 2 : FORMER

ARCHITECTES / INTÉGRATEURS / EXPLOITANTS / AUDITEURS

Les architectes, sont les personnes qui conçoivent.
Les intégrateurs, sont ceux qui installent.
Les exploitants, eux, font fonctionner au quotidien.
Les auditeurs, sont en charge du contrôle et ils vérifient l'ensemble.

Le croisement de ces catégories permet d'avoir un grand nombre de combinaisons, et pour chaque cas nous avons une palette de niveaux différents à adresser, de premier niveau à expert.

Toutes ces combinaisons donnent naissance à une multitude de métiers et de spécialités de la cybersécurité.

Liste de métiers, extraite de la page la page de recrutement de l'ANSSI (Agence Nationale de la Sécurité des SI)

AXE 2 : FORMER

Compte tenu du nombre très important de métiers de la cybersécurité, proposer dès l'origine des formations à tous ces métiers serait à la fois difficile et compliqué à mettre en place. Le but de cette filière est de répondre à un marché et à un besoin qui dans un premier temps est celui du territoire. Par exemple, ça n'aurait aucun sens de former en nombre des architectes de systèmes d'information sécurisés alors que 87 % de nos entreprises ne voient pas l'utilité d'avoir un pare-feu.
Les formations au hacking éthique sont séduisantes et peuvent palier au manque d'attractivité de nos métiers évoquée précédemment. En effet les formations à la gestion de la sécurité de l'information, permettant de maitriser la mise en place d'un SMSI (système de management de la sécurité de l'information), de mettre en application la norme ISO 27001, etc. ne font généralement pas rêver. Mais curieusement, les formations permettant de devenir hacker suscitent tout de suite plus d'intérêt !

Notre choix s'est donc porté sur des formations au hacking éthique.
Les principales raisons de ce choix sont les suivantes :

- Ce type de formation permet d'atteindre un premier niveau de connaissance sur un périmètre assez large,
- Les formations au hacking sont séduisantes ! Et le manque d'attractivité de nos métiers a été évoqué précédemment.

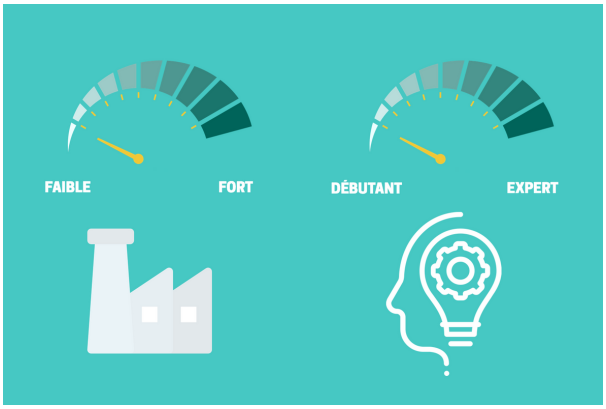
Un travail important a été réalisé pour la partie formation et en alliant les ressources de plusieurs membres d'OPEN, nous sommes dès maintenant en mesure de former et de mener les apprenants à la certification professionnelle en s'appuyant uniquement sur des ressources disponibles localement.
La gamme de formations disponible va de la sensibilisation aux bonnes pratiques pour n'importe quel salarié ou futur salarié jusqu'à la formation pour des profils de type RSSI (responsable de la sécurité des systèmes d'information) en passant bien entendu par le hacking éthique.

AXE 3 : STIMULER LA DEMANDE

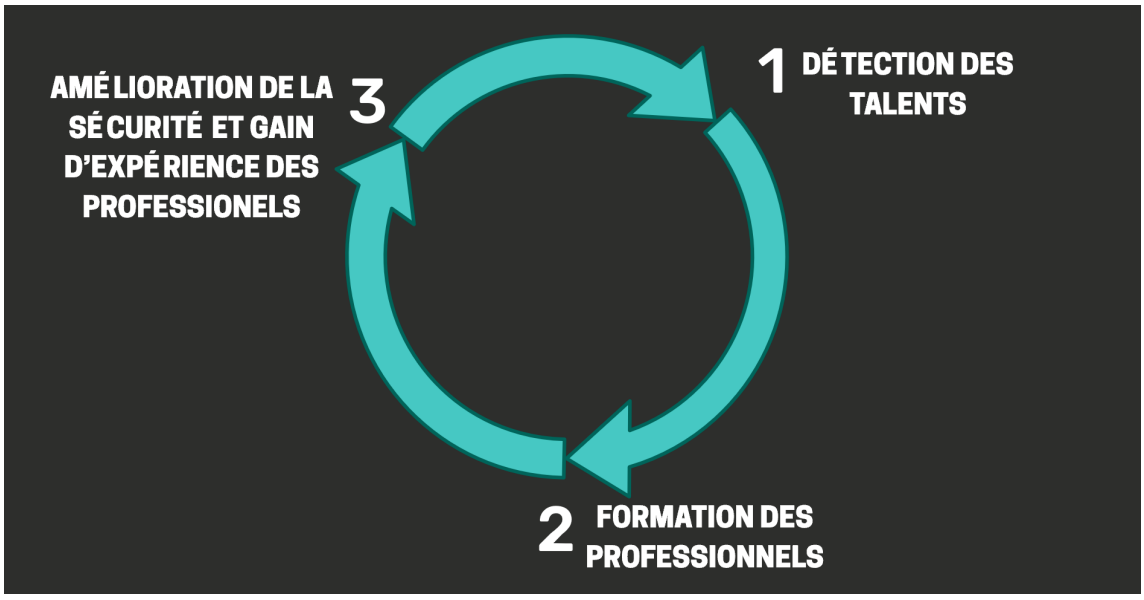
Après avoir donné envie à des calédoniennes et des calédoniens et les avoir formés, il faut que ces professionnels de premier niveau exercent leurs talents et gagnent en expérience. Comme nous avons vu précédemment que 87 % des entreprises ne sont pas convenablement protégées il reste à trouver comment les inciter à franchir le pas et qu'elles commencent à améliorer leur sécurité. Sur ce sujet aussi des travaux sont en cours au sein d'OPEN avec la création d'un dispositif incitatif du type passeport numérique ou chèque numérique, qui devrait permettre aux entreprises de s'engager sur la voie d'une meilleure protection. D'autres travaux visent à recenser les organismes qui peuvent être prescripteurs sur le sujet, comme les assurances qui peuvent inciter leurs clients à faire ce qu'il faut pour minimiser leur risque cyber.

AXE 3 : STIMULER LA DEMANDE

La demande étant ainsi stimulée, les professionnels de la cybersécurité vont pouvoir accompagner les entreprises dans l'amélioration de leur sécurité, ce qui va leur permettre de gagner en expérience. On s'inscrit alors dans une dynamique vertueuse gagnant-gagnant.
Parmi ces professionnels, certains souhaiteront probablement développer leurs nouvelles compétences à des niveaux d'expertise plus élevés ou se diriger vers d'autres spécialités de la sécurité informatique (management, audit, etc.)



Nous nous retrouvons alors dans la même logique que la première étape, avec la détection de ces talents, qui nous permettra d'enchaîner sur un 2e cycle. Et ainsi de suite vers une filière de plus en plus performante à la fois en termes de niveaux d'expertise que de variété dans les spécialités.



4e PARTIE

LES PERSPECTIVES

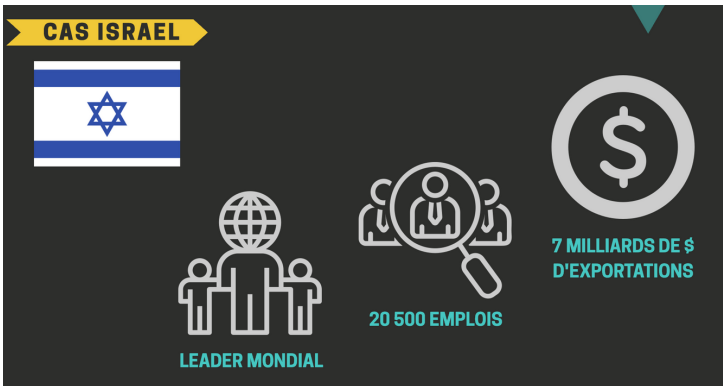
LES MARCHÉS A APPRÉHENDER

Après une première phase de développement de la filière, nous avons répondu au moi
partiellement au marché local et nous avons des équipes de professionnels avec une
expertise.

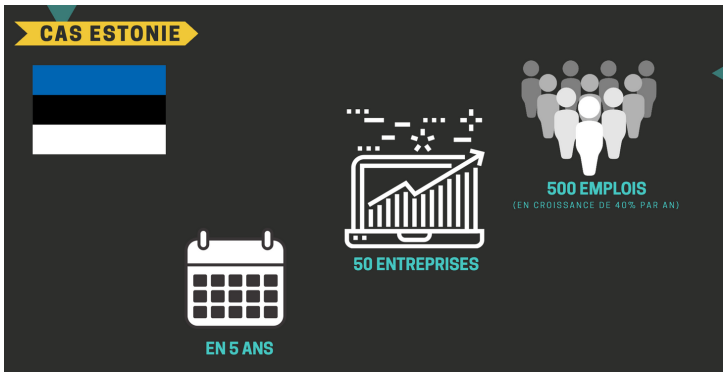
Une question se pose assez naturellement : dans ce qu'on pourrait appeler une stratég
l'après nickel, est-il réaliste que cette filière puisse exporter son savoir-faire et conqu
marchés dans la région, et pourquoi pas dans le monde ?

Pour essayer de répondre à cette question des perspectives, examinons quelques exemples de pays qui ont fait le choix de développer cette filière.

DES CAS CONCRETS



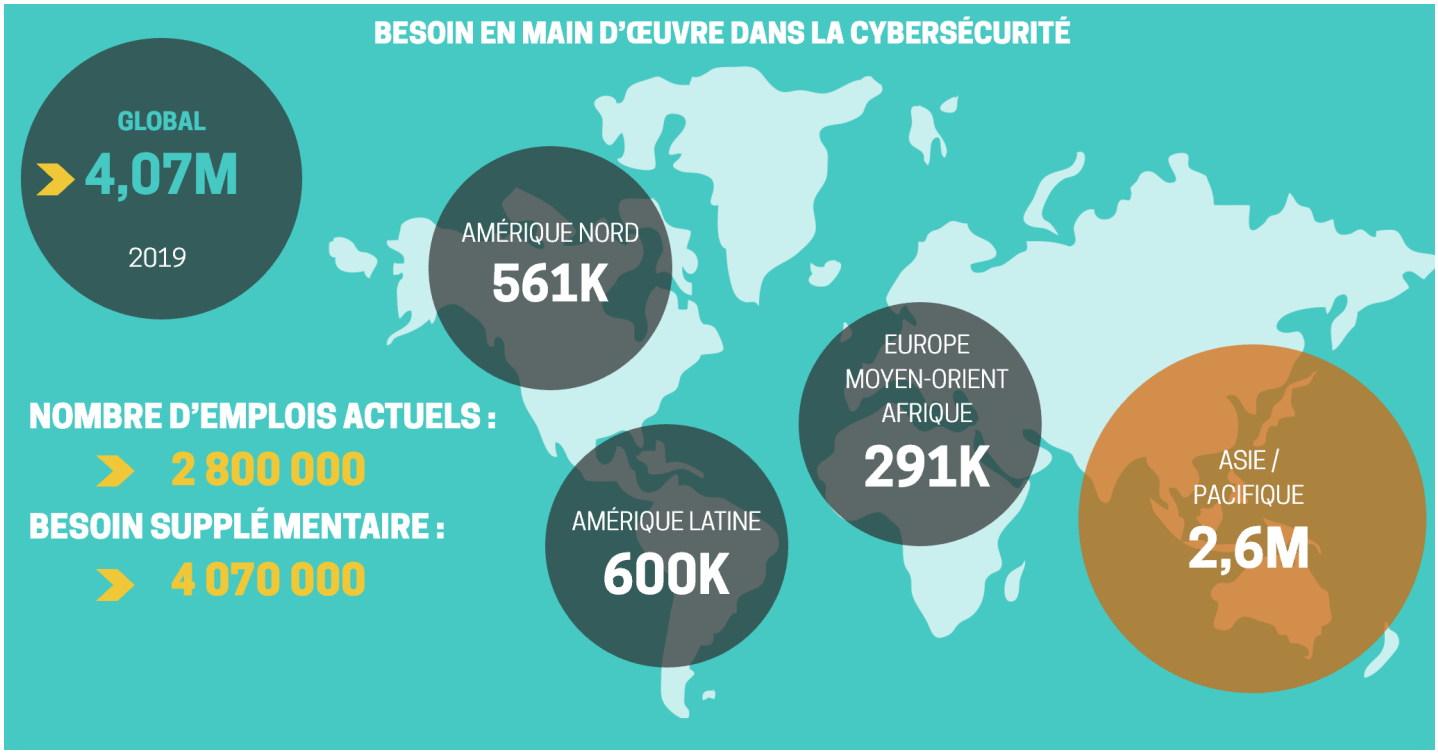
Israël est un pays leader dans le domaine de la cybersécurité, avec plus de 20 000 emplois dans le secteur et près de 7 milliards de $ d'export par an (pour un global de 110 milliards de $ pour toutes les exportations du pays). Il n'est pas question de se comparer à Israël. Dans leur cas le contexte géopolitique fait qu'ils ont estimé que développer ce secteur était une question de survie. Cependant, ils ont fait le choix de s'investir dans le secteur et c'est une belle réussite.



L'Estonie est connue pour être un état numérique, mais aussi pour être le premier état au monde à avoir subi une cyber attaque massive sur l'ensemble du pays. C'était en 2007 et ça a impacté toute l'Estonie pendant plusieurs semaines. Fort heureusement le pays s'en est relevés et les estoniens ont décidé depuis d'investir dans la cybersécurité. La encore des résultats intéressants, sur 5 ans, on note la création d'une 50e entreprises ce qui représente environ 500 emplois et c'est un nombre qui croit chaque année.

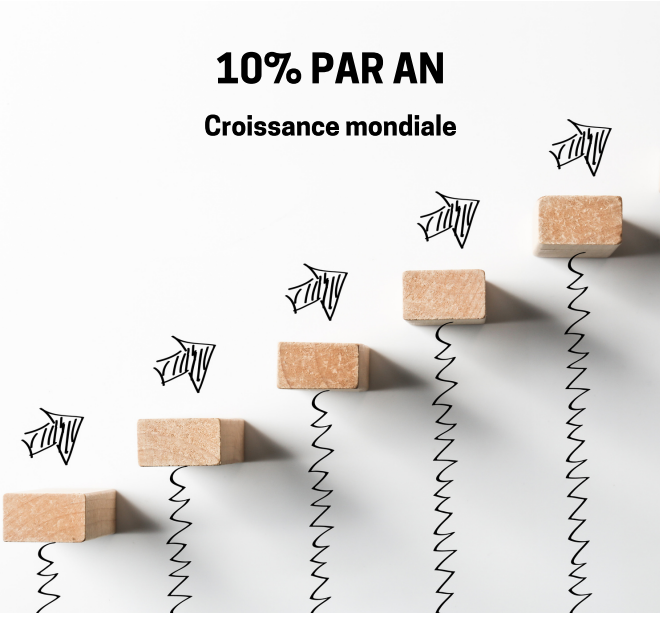
UN MANQUE DE MAIN D'OEUVRE

Le marché de la cybersécurité est en pleine expansion. Un des indicateurs qui nous a marqué est le manque chronique de main d'œuvre spécialisée.



Dans une étude de 2019, on notait que le nombre de postes à pouvoir dans le monde était de plus de 4 millions pour un nombre de professionnels actifs de 2,8 millions.
En 2019, nous avions donc 2 800 000 personnes en activité et il en aurait fallu 4 millions de plus !
Détail qui à son importance, une grosse partie de ce besoin est concentré dans notre zone (2 600 000 personnes.)
La même étude mais datée de 2018 permet de mettre en évidence qu'en à peine 1 an, nous sommes passés d'un besoin mondial d'un peu moins de 3 millions à plus de 4 millions de professionnels. La tendance est donc claire.

DES BELLES CROISSANCES



On peut également noter que la croissance moyenne dans le secteur au niveau mondial est de l'ordre de 10 % par an, mais beaucoup plus intéressant, c'est ce qui se passe dans les pays émergents en cybersécurité, c'est à dire ce qui s'y se sont mis il y a peu.

Dans ce cas, les croissances sont très rapides. L'Inde a retenu notre attention avec ses prévisions de croissance pour le secteur de la cybersécurité à horizon 2025 estimées à 775 %.

5e PARTIE

QUESTIONS-RÉPONSES

QUESTIONS - REPONSES

Et ne faut-il pas sensibiliser tous les lycéens/étudiants aux cyber risques, quels que soient les métiers envisagés ?

Si absolument et même au-delà. Une bonne hygiène de vie numérique concerne tous les utilisateurs des outils numériques.

L'Hygiène informatique en mode cloud est à la charge de l'hébergeur. Que faut-il appliquer dans ce cas ?

En mode cloud, l'hygiène informatique n'est qu'en partie à la charge de l'hébergeur (par exemple, il ne peut pas assurer l'utilisation de bon mot de passe), mais surtout les données restent de la responsabilité du propriétaire, d'où l'importance de comprendre les enjeux et les mesures mises en place par l'hébergeur.

Les forces de l'ordre et différentes institutions administratives sont-elles à même de répondre à ces menaces, que ce soit pour les pro ou les particuliers ?

A notre connaissance, les forces de l'ordre présentes sur le territoire relaient toute ou partie des plaintes vers les services concernés en France métropolitaine. A noter qu'il y a actuellement des personnels compétents sur le sujet cyber au sein de la gendarmerie et de la police nationale.

Les data centers disposent-ils de la sécurité suffisante ?

Les data centers offrent très souvent une meilleure sécurité que l'informatique installée dans une entreprise. Par contre, il faut prendre conscience que la sécurité du data center s'arrêtent aux murs de celui-ci, elle n'est pas extensible à l'entreprise et aux utilisateurs.

Quel est le poids du Darkweb par rapport à la cybersécurité ?

Le Darkweb au sens marché noir illégal propose énormément de services destinés aux attaquants informatiques et même au-delà avec des produits illégaux. Ce marché est la principale source d'approvisionnement des organisations cybercriminelles.

QUESTIONS - REPONSES

Comment se protéger pour que les personnes formées ne deviennent pas les meilleurs hackeurs de NC ?

Réponse par une autre question : comment se protéger pour que les personnes formées à la serrurerie ne deviennent pas les meilleurs cambrioleurs de NC ? Les formations au hacking éthique abordent explicitement le sujet de l'éthique. L'objectif est bien de proposer aux futurs professionnels de pratiquer le hacking dans le cadre de la loi ; d'être remercié par leurs clients et payé pour cela.

Vous dites être autonome sur des formations... concrètement, c'est quoi ? Vous avez ouvert des sessions de formations ? C'est payant ? Gratuit ?

En regroupant les ressources d'au moins 3 membres d'OPEN, nous sommes en mesure de proposer des formations certifiantes en mode présentiel. Ces formations sont éligibles aux mesures de financement de la formation professionnelle (FIAF). Il n'y a pas de sessions de planifiées pour l'instant. Notre but était dans un premier temps de s'assurer de la faisabilité : disponibilité de l'organisme de formation déclaré DFPC, d'au moins 1 formateur agréé DFPC, du centre de formation certifié et agréé EC-Council, d'au moins 1 formateur certifié et agréé EC-Council, de salles de formation répondant aux requis techniques, d'un centre d'examen pour les certifications et de l'autorisation d'utiliser les supports de cours officiels EC-Council. Les formations sont payantes mais peuvent être prises en charge dans le cadre du Fond Interprofessionnel d'Assurance Formation.

Comment nous positionnons-nous en termes de compétences par rapport à nos voisins du pacifique ?

C'est difficile à dire car nous n'avons pas de recensement fiable des compétences disponibles en Nouvelle-Calédonie. Si on se base sur les personnes certifiées CISSP par exemple :

141 607 dans le monde - 1 105 en France - 2 en Nouvelle-Calédonie - 1 en Polynésie Française - 2 750 en Australie - 337 en Nouvelle-Zélande

Cependant, il existe de nombreuses certifications et un professionnel compétent n'est pas forcément certifié.

QUESTIONS - REPONSES

Quelles sont les formations initiales et continues existantes aujourd'hui en NC et hors NC ? Existe-t-il des formations accessibles 100% en ligne ?

A notre connaissance, il n'y a pas de parcours de formation complet disponible sur le territoire. Les formations dédiées entièrement à la cybersécurité peuvent être trouvées sur le site de l'ANSSI et sont reconnues avec le label SecNumEdu : https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/.

Un des objectifs d'OPEN, au-delà des formations professionnelles déjà disponibles en présentiel sur le territoire et de compléter l'offre avec des formations hybrides accessibles depuis n'importe quelle zone du territoire.

Le pare feu Windows est-il efficace ?

Comme tous les pare-feux, pour être efficace, il doit être correctement configuré et être à jour.

Mais n'y a-t-il pas un pare-feu par défaut dans les modems ?

Un modem traduit un langage de communication dans un autre. Par définition, il n'y a pas de mécanismes de filtrage que l'on peut attendre d'un pare-feu. Malgré tout, certains modems peuvent inclure des fonctions basiques de filtrage et certains pare-feux plus avancés peuvent inclure un modem. Il faut effectivement choisir le matériel en fonction de son contexte. Pour un particulier où l'importance de la cybersécurité n'est pas capital, un modem avec des fonctions basiques de filtrage peut faire l'affaire. Par contre, pour une entreprise, il faut s'équiper de pare-feu dédié, surtout s'il y a plusieurs équipements informatiques (ordinateurs, NAS, serveur, imprimante réseau, smartphones des employés ou des invités)

C'est quoi un pare-feu ?

Un pare-feu est une sorte de filtre. Il analyse le trafic réseau et en fonction de son paramétrage élimine les communications interdites ou suspectes.

QUESTIONS - REPONSES

Ou peut-on trouver la liste pour faire le check up et l'hygiène informatique ?

Pour les particuliers et les petites entreprises : https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/

Pour les entreprises où les données sont plus importantes : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

On parle de cybersécurité mais combien de cas avérés en NC ?

D'après une étude de l'Observatoire du Numérique, 25% des entreprises en Nouvelle-Calédonie ont déjà subi un incident de sécurité en 2018. Cela équivaut à environ 10 000 cas avérés rien que pour les entreprises. A l'heure actuelle, ce chiffre est sans aucun doute plus important.

Quel est l'indice CRI pour l'Estonie, le « royaume » du tout numérique ? S'il est proche de 0, quelles sont leurs solutions de protection ?

Indice de 0,456, juste en dessous de celui de la France (0,457).

Comme vous avez pu le faire par l'exemple du phishing, ne pensez-vous pas qu'il s'agit en premier lieu de travailler sur la cyber-éducation ?

La sensibilisation aux bonnes pratiques et la mise en place des protections de base (anti-virus, pare-feu, mots de passe, mises à jour, sauvegardes) sont complémentaires. Porter sa ceinture de sécurité en voiture est capital, mais conduire prudemment en respectant les bonnes pratiques l'est tout autant. Idem pour la cybersécurité.

Les entreprises sont-elles prêtes à payer pour la cybersécurité ?

C'est un des axes de travail dans la mise en place de cette filière : comment inciter et stimuler la demande des entreprises pour l'amélioration de leur niveau de sécurité.

Un rgs NC est en cours d'élaboration. Participez-vous à cette réflexion ?

Non.

Note : RGS = Référentiel Général de Sécurité.

QUESTIONS - REPONSES

Est-ce que la crypto-monnaie est une option digitale de paiement fiable ?

Oui sur le plan technique. Le principal défaut des crypto-monnaies aujourd'hui est leur volatilité et le faible nombre d'acteurs économiques qui les reconnaissent.

Est-ce que nos institutions sont sensibilisées à la question ?

Etaient représentés lors de l'OPEN MEETING, le Gouvernement de la NC, la Province des Iles et la Province Sud. Ca nous semble être une bonne indication de leur intérêt.

Pourquoi ne fait-on pas venir de modem sécurisé ?

Chacun est libre (grossistes, revendeurs, utilisateurs) de commander et d'acheter les équipements qu'il souhaite en fonction de ses besoins et ses contraintes.

Quels sont les pays dans le monde, d'où partent les attaques cyber ?

Les attaques sont souvent envoyées par des passerelles (proxy, bot…) disséminées partout dans le monde, y compris en Nouvelle-Calédonie. Les commanditaires derrière ces attaques sont par contre plus complexes à déterminer, sachant qu'il y a plusieurs types d'attaquants (cybercriminel, étatique, activiste…).

Est-ce que les formations seront disponibles à distance ? Sous quelles formes ?

A terme oui. L'objectif est que les apprenants situés sur tout le territoire puissent accéder aux formations.

Hacking éthique ok mais il faut les former à contrer les failles trouvées.

Oui. L'objectif du hacking éthique est de mettre en place des protections et contremesures en mettant à profit son expertise dans l'utilisation des techniques et des outils de hacking. Par exemple pour respecter les bonnes pratiques dans le cas d'un test d'intrusion (pentest), l'auditeur se doit de proposer des solutions permettant d'éliminer ou de minimiser les impacts des failles qu'il a exploité.

QUESTIONS - REPONSES

13% tout confondu particuliers et entreprises ?

Ce pourcentage est celui des entreprises qui utilisent un pare-feu. Il provient d'une étude publiée par l'ONNC (Observatoire Numérique de Nouvelle-Calédonie) en 2018.

Quel sera l'impact au niveau cyber / interception de données avec la mise en place du futur câble sous-marin de l'OPT à destination de Fiji (cf. Huawei/Chine) ?

Sur le plan purement technique, ça enlèvera un point unique de panne (1 seul câble actuellement) et ajoutera un point de fuites d'informations potentielles. Le fait que ce câble passe par Fidji n'a d'impact que pour des considérations stratégiques et géo politiques, sachant qu'actuellement les pays occidentaux estiment qu'il est acceptable que leurs données soient interceptées, stockées et analysées par les Etats-Unis et qu'il est inacceptable qu'elles le soient par la Chine.

Le profil type du cyber protecteur est un homme de 45 ans + mais quel est le profil type du cyber attaquant ?

Il faudrait consulter les services de renseignement à ce sujet.

Les anti-spam permettent d'isoler les adresses mails des spammeurs (temporairement). Pourquoi en amont les FAI ne bloquent-ils pas les IP des hackeurs ?

Certains le font, mais cela pose des problèmes de censure. De plus les hackeurs utilisent toujours des systèmes pour masquer leur réelle adresse IP publique.

La cyber sécurité est-elle une affaire de geeks ?

Non. Ni pour devenir un professionnel du sujet, ni pour être un utilisateur éclairé.

Quel est le niveau de maturité des entreprises calédoniennes ?

Si on se réfère aux baromètres numériques de l'Observatoire du Numérique de Nouvelle-Calédonie, il est faible mais en amélioration.

QUESTIONS - REPONSES

Il paraît que la NC est parmi les pays les plus attaqués... est-ce vrai ? Quels sont les chiffres ?

Pour évaluer les attaques en Nouvelle-Calédonie, il faut prendre en compte tous les types d'attaques, en corrélation avec d'autres indicateurs et les comparer aux autres pays. Les données ne sont pas encore suffisantes pour obtenir un chiffre précis. Mais la tendance des indicateurs de risque cybercriminel montre que la Nouvelle Calédonie est plus attaquée que la majorité des pays.

Et pourtant l'Inde était dernier pays sur le classement des pays les plus attaqués !

Oui, l'Inde est classée dernier en termes de risque d'attaques de cybercriminalité. En effet, la population de l'Inde est très peu équipée en numérique et c'est une population pauvre, d'où le « désintérêt » des cybercriminels. Il faut bien comprendre que ce classement ne prend pas en compte les attaques dites étatiques ou militaires.

Il y a aussi plus de 50% qui ont un niveau supérieur à Bac+3 ...

38% avec un niveau supérieur à bac+3.
Attention, notre propos n'est pas de dire qu'il ne faut pas ou qu'il n'y a pas de professionnels très diplômés dans le secteur, mais qu'il n'est pas nécessaire d'avoir un haut niveau de formation initiale pour trouver sa place dans la cybersécurité.

Les certifications CISSP peuvent être passées dans un centre de certification Pearson Vue. Il y a 1 centre en Nouvelle-Calédonie

Merci de l'info, c'est une bonne nouvelle.
Note : le site de Pearson Vue a un problème de référencement du centre d'examen de Nouméa (SF2I). Cela devrait être bientôt réglé ce qui permettra d'y avoir accès lors d'une demande de passage d'examen de certification CISSP.

C'est comme pour le covid il y en a peut-être moins que dans le reste du monde mais il y en a quand même et il faut se protéger pour empêcher la propagation.

En effet, cybersécurité est un enjeu global et collectif.

contact@open.nc
73.11.60
www.open.nc

OPEN
.NC