F cyber A2
MH/JC/JP
845-2021

Bruxelles, le 6 mai 2021

AVIS

sur

LA POLITIQUE GOUVERNEMENTALE RELATIVE À LA CYBERSÉCURITÉ DES PME

(approuvé par le Bureau le 16 février 2021,
entériné par l'Assemblée plénière du Conseil Supérieur le 6 mai 2021)

Conseil Supérieur des Indépendants et des PME
North Gate II (4ème étage) - Boulevard du Roi Albert II 16 - 1000 Bruxelles
Tél. : 02 277 90 16 - cs.hr@economie.fgov.be - www.csipme.fgov.be

La cybersécurité constitue un défi majeur pour les indépendants et les PME. Par conséquent, le Conseil Supérieur des Indépendants et des PME a décidé d'émettre un avis d'initiative sur la politique gouvernementale relative à la cybersécurité des PME. Après des discussions au sein de la commission ad hoc " Cybersécurité ", le Bureau du Conseil Supérieur a émis le 16 février 2021 l'avis suivant, entériné par l'Assemblée plénière du Conseil Supérieur le 6 mai 2021.

INTRODUCTION

1. Une priorité politique importante

La cybercriminalité constitue une menace réelle pour les indépendants et les PME, qui de surcroît, sont très peu protégés. Pourtant, la cybercriminalité peut coûter très cher à une entreprise, voire même compromettre sa pérennité. Tant la cybercriminalité que les mesures de protection contre ce phénomène occasionnent des frais importants aux entreprises et à l'économie belges. Dans le cadre du Règlement général sur la protection des données et des obligations qu'il impose aux PME, la cybersécurité joue également un rôle primordial. La cybersécurité et, plus généralement, la confiance numérique constituent en outre des conditions importantes à une digitalisation plus poussée de notre économie ainsi qu'à la croissance de l'économie numérique. La cybersécurité des indépendants et des PME est ainsi devenue, à juste titre, une priorité politique essentielle. Il convient de continuer à y consacrer des efforts.

2. Un problème complexe

L'amélioration de la cybersécurité des entreprises est un problème complexe à multiples facettes qui concerne, en outre, de nombreux acteurs.

D'une part, on peut distinguer la lutte contre la cybercriminalité et d'autre part la protection contre la cybercriminalité ou l'amélioration de la cyberrésilience des entreprises. Un large éventail de défis économiques, juridiques, technologiques, sociaux et éthiques se posent. La cyberprotection au sein d'une entreprise a à la fois une composante technologique et une composante humaine importante (ladite "erreur humaine"). Il faut aussi souligner que la cybercriminalité est un problème de nature internationale et transfrontalière.

De nombreux acteurs privés et publics sont associés à la lutte contre la cybercriminalité et à la cyberprotection. Les PME elles-mêmes ne sont pas seulement considérées comme des victimes (potentielles), mais également comme coresponsables de leur propre protection et de la protection de leurs clients, leur personnel et leurs partenaires. Les fournisseurs, les prestataires de services, les clients et les membres du personnel ont également un rôle à jouer dans ce cadre. S'agissant des acteurs publics, plusieurs domaines et niveaux politiques sont concernés. Toutefois, l'implication de nombreux acteurs ne constitue pas nécessairement un désavantage : cela peut tout autant représenter une opportunité de mobiliser des ressources et des efforts importants. Un niveau minimum d'harmonisation et de coopération est cependant nécessaire pour y parvenir.

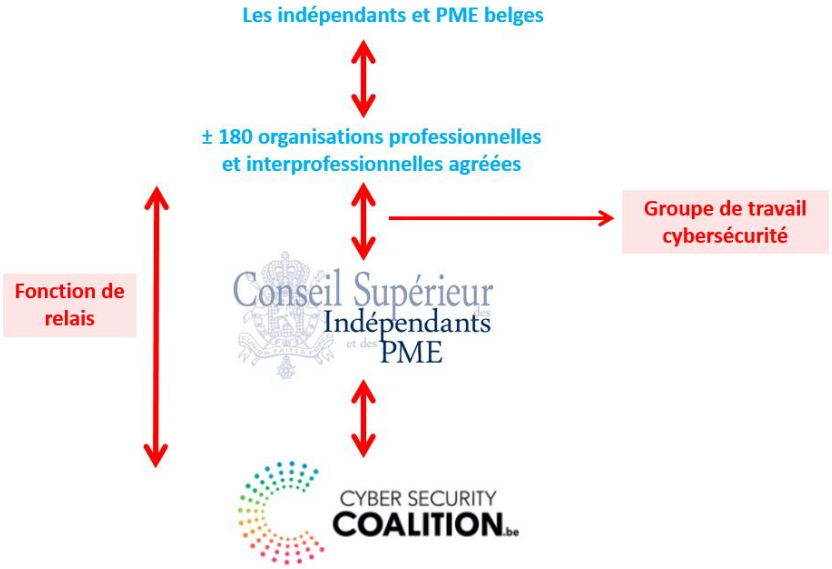
3. Rôle actif du CSIPME et de ses membres

Le Conseil Supérieur des Indépendants et des PME et les organisations professionnelles et interprofessionnelles agréées représentées en son sein contribuent également à l'amélioration de la cybersécurité des indépendants et des PME.

Depuis janvier 2018, le Conseil Supérieur est membre de la Cyber Security Coalition (CSC) belge, dans le cadre de laquelle des organisations publiques, des entreprises et les milieux universitaires unissent leurs forces. En effet, la question d'une meilleure représentation des PME au sein de la CSC s'est posée. Il est ressorti de la concertation entre les acteurs concernés qu'il conviendrait que le Conseil Supérieur joue un rôle dans ce cadre. Pour ces raisons, le Conseil Supérieur est devenu membre de la CSC. Le secrétariat du Conseil Supérieur représente, dans la CSC, les organisations professionnelles et interprofessionnelles représentées en son sein et joue un rôle de liaison entre ces dernières et la CSC. En plus, ces organisations peuvent également s'affilier à la CSC de manière individuelle et bénéficier ainsi des avantages directs de l'affiliation. Concrètement, l'adhésion du Conseil Supérieur à la CSC se traduit par une participation active aux activités et aux différents *focus groups* de la CSC.

En interne, le Conseil Supérieur a établi un groupe de travail permanent "Cybersécurité" (sous forme d'une commission ad hoc), réunissant des représentants de plusieurs organisations professionnelles et interprofessionnelles représentées en son sein. L'objectif principal de ce groupe de travail est d'améliorer la cybersécurité des indépendants et des PME. À cette fin, il s'est fixé les sous-objectifs suivants : préparer des points de vue ; soutenir la fonction de relais CSIPME-CSC ; acquérir de l'expertise ; promouvoir la collaboration et aider les autres acteurs dans leurs efforts pour assurer la cybersécurité pour les PME

Le schéma ci-dessous montre les relations de coopération susmentionnées.



Le Conseil Supérieur et ses membres mènent également des actions à des fins d'information, de sensibilisation et de soutien des indépendants et des PME dans le domaine de la cyberprotection, par exemple en organisant des séances d'information, en diffusant les instruments de la CSC ou encore en collaborant aux campagnes du Centre pour la Cybersécurité Belgique.

Vision de la cybersécurité des PME

L'intention du présent avis n'est pas de proposer un plan d'action détaillé reprenant les mesures qui devraient être prises par les autorités afin d'améliorer la cybersécurité des indépendants et des PME. Via son avis, le Conseil Supérieur souhaite avant tout faire part de sa vision de la cybersécurité des indépendants et des PME et, plus particulièrement, de la politique gouvernementale y afférente. Les principes, lignes directrices et points d'attention dont il convient de tenir compte dans le cadre de cette politique sont donc formulées ci-dessous, ainsi que quelques propositions d'action concrètes.

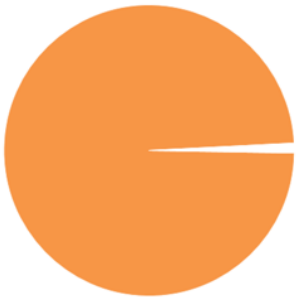
1. Un problème réel

La cybercriminalité constitue un problème réel pour les indépendants et PME belges. Les chiffres disponibles mettent en évidence non seulement la gravité du problème mais également le fait que les risques augmentent d'année en année. Or, les PME sous-estiment ces risques. En général, elles ne se considèrent pas comme une cible pour les cybercriminels. Contrairement à la criminalité physique, la cybercriminalité est beaucoup moins visible. De plus, les entrepreneurs devenus victimes de la cybercriminalité ont moins tendance à communiquer à ce sujet, craignant une détérioration de leur image et une perte de confiance de leurs clients et partenaires.

Par conséquent, il est nécessaire d'informer et de sensibiliser les PME de manière permanente sur le risque encouru. Une des actions concrètes dont le Conseil Supérieur est partisan, consiste en une campagne d'information construite autour de témoignages des PME victimes de cybercriminalité. Il est également important d'accroître la volonté des PME de signaler les incidents. Une bonne collecte de données sur les cyberincidents et une typologie commune utilisée par tous les acteurs aideraient également à mieux identifier les cyberincidents auxquels sont confrontées les PME et donc à convaincre ces dernières des risques encourus.

2. La grande majorité des entreprises sont des petites entreprises

Quand on évoque la cybersécurité et, plus généralement, la digitalisation, on perd souvent de vue que la grande majorité des entreprises belges sont des petites entreprises. En outre, il faut relever que la plupart d'entre elles ne dispose pas de son propre responsable TIC. 99 % des entreprises belges ont moins de 50 salariés. D'après la définition européenne, les PME sont des entreprises qui occupent moins de 250 salariés. Dans le contexte belge, ce concept renvoie toutefois généralement à des entreprises qui occupent moins de 50 salariés et qui sont, par conséquent, désignées comme des petites entreprises dans la définition européenne. De plus, les chiffres repris ci-dessous montrent que beaucoup de ces entreprises sont des microentreprises occupant moins de 10 employés, voire aucun employé. Il en résulte que dans le cadre d'une initiative politique visant les entreprises, les PME devraient être le point de référence et la norme (conformément au principe européen « Think small first »). En tout état de cause, il convient de prévoir un nombre suffisant d'initiatives visant spécifiquement ce groupe important de petites entreprises.



99 %

des entreprises belges sont des PME (< 50 salariés)

97 %

97% des entreprises belges sont des micro-entreprises (< 10 salariés)

	Nombre d'entreprises	%
Sans salariés	823.345	81,5%
1-4 salariés	121.306	12%
5-9 salariés	30.347	3%
10-19 salariés	17.332	1,7%
20-49 salariés	11.175	1%
50-249 salariés	5.513	0,6%
+250 salariés	1.617	0,2%
Total	1.010.635	

Source: bestat.statbel.fgov.be – En date du 8/10/2020

En outre, la part des entreprises numériques et de haute technologie est surestimée dans certains domaines politiques. Certes, ces entreprises méritent une forte attention politique et dans d'autres secteurs, il n'y a pas d'entreprise en dehors de tout processus plus ou moins élaboré de digitalisation. Toutefois, la plus grande partie de notre économie se compose d'entreprises et de professions non-numériques et non-technologiques, allant des courtiers d'assurance aux entreprises de construction. Ces entreprises sont également confrontées à des défis relatifs à la cybersécurité. Il convient de ne pas perdre de vue cet élément lorsque des initiatives visant à améliorer la cybersécurité des entreprises sont prises.

Enfin, il convient de souligner que les PME varient fortement entre elles, tant au niveau de leur taille que du type d'activité, du degré de digitalisation, de la maturité en matière de cybersécurité, du profil de risque et de la manière dont elles sont organisées. Au sein du groupe des PME, une segmentation plus poussée sera donc nécessaire.

3. Situation spécifique des PME

En termes de cybersécurité, les indépendants et PME se retrouvent dans une situation particulière. Par conséquent, ils ont besoin d'un soutien supplémentaire de la part des autorités.

- En premier lieu, force est de constater que la PME moyenne est mal protégée, surtout en comparaison avec les entreprises et organisations de plus grande taille, ce qui fait d'elle une cible facile.

- En plus, il peut être observé que les entreprises et organisations plus grandes se protègent de mieux en mieux et que, par conséquent, les cybercriminels se concentrent davantage sur les acteurs moins protégés, notamment les PME.

- En outre, les cybercriminels considèrent les petites entreprises comme une porte d'entrée vers les entreprises et organisations de plus grande taille. S'ils n'arrivent pas à se procurer un accès direct aux grands acteurs, ils essaieront de les atteindre via les petits partenaires moins protégés qui sont connectés aux grands acteurs via l'internet.

- Vu leur petite taille, les PME ne disposent souvent pas de leur propre service TIC ou d'expertise TIC interne. Pour leurs besoins en la matière, elles doivent donc faire appel à des prestataires de services externes, ce qui peut également entraver la mise en œuvre de mesures de cybersécurité.

- Les PME sont également confrontées à des désavantages d'échelle. Des mesures techniques telles que l'installation d'un pare-feu ont un coût presque identique pour les grandes et les petites entreprises. Par rapport à la taille de l'entreprise, la cyberprotection sera donc plus chère pour les petites entreprises.

- En raison de leur petite échelle, les petites entreprises éprouvent en outre davantage de difficultés à surmonter les conséquences d'un cyberincident. Un cyberincident aura sur elles un impact plus important, vu qu'elles sont plus petites et disposent de moins de réserves pour pallier aux effets d'un tel incident.

- Enfin, il y a la constatation simple que les PME sont plus nombreuses que les grandes entreprises. Logiquement, il s'ensuit que beaucoup plus de petites que de grandes entreprises sont touchées par la cybercriminalité.

Par conséquent, il est d'une importance primordiale que les autorités accordent une attention suffisante et spécifique aux PME dans le cadre de leurs politiques de cybersécurité.

4. Sensibilisation et formation à la mesure des PME

Le Conseil Supérieur est convaincu que la cybersécurité doit constituer une priorité pour les indépendants et PME, mais l'entrepreneur lambda reçoit des quantités d'information énormes et a de nombreuses préoccupations prioritaires, allant de la réduction du nombre d'accidents de travail à la lutte contre la fraude sociale. Par conséquent, le Conseil Supérieur plaide pour une approche pragmatique à la mesure des PME, mettant l'accent sur la prévention, la sensibilisation et la formation et permettant aux PME de réaliser effectivement des avancées vers une meilleure cybersécurité.

Il convient de prendre en considération les différentes fonctions ou domaines de travail de la cybersécurité (*identify, protect, detect, respond, recover*), tout en mettant l'accent avant tout sur des actions protectrices et préventives.

Outre des solutions technologiques et axées sur les processus qui soient qualitatives et abordables à la mesure des PME, il y a lieu d'accorder une attention particulière au facteur humain. En misant pleinement sur la sensibilisation et la formation, une cyberhygiène de base peut être poursuivie et un investissement relativement limité en temps et en ressources permettra d'améliorer sensiblement la cybersécurité de l'entreprise. Pour les PME, il reste toutefois beaucoup à faire en matière de sensibilisation et de formation. Il convient en outre de tendre vers un changement de comportement concret de la part des entrepreneurs et de leur personnel. Pour ce faire, on pourrait avoir recours aux connaissances issues de la psychologie comportementale et à des techniques comme le *nudging* et la *gamification*.

Les informations et instruments doivent être créés à la mesure des PME.

- Le langage, la quantité et la complexité des informations doivent être adaptées. Quand il s'agit, par exemple dans une brochure d'information, de *management commitment* et il est fait référence aux différentes fonctions de management, on n'est pas en phase avec la réalité de la PME belge moyenne. Par conséquent, on court le risque que de nombreuses PME décrochent immédiatement.

- À l'heure actuelle, les informations pertinentes pour les PME en matière de cybersécurité sont éparpillées à plusieurs endroits. Il serait toutefois plus commode pour les PME que toutes les informations utiles relatives à leur cybersécurité soient regroupées sur un seul site web.

- Les PME ont besoin d'informations et d'outils concrets et pratiques. La plupart d'entre elles ont très peu d'expertise TIC interne et certainement pas dans le domaine de la cybersécurité. Souvent, elles ne disposent pas non plus des moyens de faire appel, de manière intensive, à un prestataire de services externe. Bref, il est peu utile de demander aux PME d'utiliser des outils ou de prendre des mesures irréalisables vu qu'elles ne disposent pas de l'expertise nécessaire à cet effet ou qu'il est trop coûteux de faire appel à un soutien extérieur. Pour les actions qui sont nécessaires et qui requièrent une expertise spécifique, les autorités devraient prévoir des mesures de soutien (déductibilité fiscale, chèques-conseil, …). Les scans ou auto-évaluations conseillant aux PME de prendre certaines mesures pourraient également proposer aux PME sans expertise TIC interne une check-list qu'elles peuvent utiliser pour chercher un prestataire de services et entamer le dialogue avec ce dernier.

Comme mentionné précédemment, les PME ne constituent pas un groupe homogène. Dans la mesure du possible, la situation individuelle de chaque entreprise devrait être prise en considération, par exemple en partant de la situation concrète de l'entreprise concernée dans le cadre des scans ou des outils d'évaluation. A tout le moins, il conviendrait de tenir compte des caractéristiques similaires des entreprises actives dans le même secteur professionnel, par le biais d'une approche spécifique à la profession (cf. infra).

En ce qui concerne la certification de la cybersécurité des PME, le Conseil Supérieur prône une approche prudente et mesurée. En raison de leur échelle plus réduite, il est plus difficile d'obtenir un certificat pour les PME que pour les grandes entreprises. Pour la grande majorité d'entre elles, de tels certificats sont en outre peu utiles à l'heure actuelle. S'agissant des PME, il conviendrait avant tout de miser sur une meilleure sensibilisation et information, ainsi que sur des conseils concrets sur-mesure. En tout état de cause, la certification doit être facultative et les initiatives publiques en matière de certification devraient être axées sur les créneaux de marché où les certificats apportent une réelle valeur ajoutée vu que sans elles, les entreprises seront confrontées à des exigences divergentes de la part de leurs clients en matière de rapports ou devront présenter des certificats existants plus contraignants. De plus, les PME sont demandeuses de davantage de garanties relatives à la cybersécurité des services et produits TIC qu'elles utilisent. A cet égard, la certification des services, produits et prestataires de services TIC serait une bonne piste.

5. Miser sur des solutions technologiques

Les stratégies pour améliorer la cybersécurité des PME devraient viser à décharger les PME autant que possible de ces préoccupations et de ce travail. Le fait que le facteur humain (erreur humaine) joue souvent un rôle important dans les incidents de cybersécurité démontre que l'entrepreneur et son personnel feront toujours partie du tableau. D'un autre côté, cela signifie également qu'il est indiqué de limiter le facteur humain autant que possible. Il convient donc de miser sur des stratégies et technologies visant une meilleure protection de l'entrepreneur sans que celui-ci ne doive faire quoi que ce soit ou se préoccuper à ce sujet.

Prenons l'exemple du phishing : il convient de continuer à travailler sur la sensibilisation et l'information des entrepreneurs, mais il est encore mieux d'assurer que ces courriels phishing n'atteignent pas l'entrepreneur par le biais de meilleurs filtres anti-spam, en bloquant les sites web véreux de manière rapide, par le biais de la collaboration internationale visant à lutter contre les bandes à l'origine des attaques phishing, etc. L'authentification multi-facteurs et les solutions cloud peuvent également décharger l'entrepreneur de ces préoccupations. Par ailleurs, il existe de nombreuses solutions technologiques pour les grandes entreprises qui ne sont généralement pas accessibles aux PME : il s'agit par exemple de tests de phishing, des essais d'intrusion automatisés, de la protection contre les risques numériques, de la détection et réponse gérées, …

Le Conseil Supérieur préconise que les autorités prennent des mesures visant à renforcer l'offre de solutions technologiques, à les rendre appropriées et accessibles aux PME et à stimuler les PME à en faire usage. L'application récemment développée BeGuard, du Centre pour la Cybersécurité Belgique, est un exemple d'une solution technologique ciblée sur les PME qui peut se révéler très utile pour ces dernières. En outre, il convient de veiller à ce que les PME n'utilisent que des logiciels répondant à des exigences minimales de sécurité, d'où l'importance de la certification des logiciels.

6. Évaluation des risques pour une protection adaptée

Les PME ont besoin d'une cybersécurité adaptée à leurs spécificités et cyber-risques. Il importe de les convaincre de prendre les actions qui sont réalisables pour elles et renforcent effectivement leur cybersécurité. En tout cas, il convient d'éviter qu'elles investissent du temps et des ressources dans des solutions qui ne leur offrent aucune protection, une protection trop poussée ou une protection inadaptée. Voilà pourquoi il importe de savoir à quels risques les PME sont confrontées.

L'analyse simple des risques au niveau des PME individuelles peut certainement être encouragée, mais au vu des grandes similarités entre les PME actives dans le même secteur professionnel, il conviendrait certainement aussi qu'une évaluation des risques soit effectuée au niveau du secteur. Il serait également opportun pour l'ensemble des PME belges qu'une évaluation des risques soit réalisée et qu'il y ait plus d'informations fiables et détaillées sur les cybermenaces et les frais qu'elles occasionnent.

Par conséquent, le Conseil Supérieur demande aux autorités de soutenir l'élaboration d'évaluations sectorielles des risques et de veiller à ce que davantage de données fiables soient collectées sur les cybermenaces qui pèsent sur les PME belges. C'est l'une des raisons pour lesquelles il est préconisé dans le présent avis de tendre vers une meilleure collecte de données et une typologie commune en matière de cyberincidents. Davantage d'informations relatives à l'efficience et l'efficacité des actions et mesures sont également nécessaires, tant au niveau des PME qu'au niveau politique. A cet égard, il importe également d'observer comment les autres pays s'attaquent au problème de la cybersécurité des PME. Le rôle pouvant être joué par les cyberassurances pour les PME mérite également d'être considéré dans ce contexte.

7. Une approche spécifique à la profession ou au secteur

Le Conseil Supérieur est convaincu que la meilleure approche de la cybersécurité des PME serait d'avoir recours à une stratégie spécifique à la profession ou au secteur.

Les entreprises actives au sein du même secteur professionnel sont très similaires en ce qui concerne le type d'activité exercée, les types de données, la taille de l'entreprise, l'environnement TIC et la maturité en matière de cybersécurité. Par conséquent, elles auront également un profil de risque et des besoins en matière de cyberprotection similaires. Plutôt que de chercher des solutions individuelles, il conviendrait donc que les PME le fassent de manière conjointe au sein de leur secteur professionnel.

Une approche axée sur la spécificité de la profession ou du secteur permet également d'utiliser les structures de coopération et les canaux de communication existants. Les organisations professionnelles constituent un excellent partenaire pour les autorités et les PME quand il s'agit d'aider les PME à améliorer leur cybersécurité. Elles sont en contact direct avec de nombreuses PME actives dans leurs secteurs et constituent un canal de communication direct dans lequel les entrepreneurs ont confiance. De plus, les organisations professionnelles connaissent les activités professionnelles et l'environnement TIC dans le cadre desquels les PME fonctionnent. S'agissant du processus plus large de digitalisation de la PME, l'organisation professionnelle est également le partenaire par excellence.

Par conséquent, le Conseil Supérieur préconise que dans la mesure du possible, les autorités adoptent une approche spécifique à la profession ou au secteur et encouragent et soutiennent des initiatives axées sur la spécificité de la profession ou du secteur.

8. La cybersécurité en tant que partie de la digitalisation

Les PME sont confrontées d'une part au défi d'améliorer leur cyberprotection, et d'autre part, à celui posé par la digitalisation plus poussée et la transformation digitale. Pour les PME, la meilleure manière de relever ces défis serait de le faire de manière conjointe et au niveau sectoriel, dans le cadre de leur organisation professionnelle. Plutôt que de considérer la cybersécurité comme un défi isolé, elle devrait être considérée comme une composante de la digitalisation. Si l'on examine, au sein d'un secteur ou d'une profession déterminée, quel serait l'environnement numérique idéal pour une PME active dans ce secteur ou cette profession, et si l'on essaie de concrétiser cet environnement, il pourrait être examiné en même temps comment assurer une cybersécurité suffisante.

En outre, cette approche reflète le principe de *security* et *privacy par design.* Plutôt que de concevoir et de développer d'abord un environnement numérique et de réfléchir après à la manière de garantir la cybersécurité dans cet environnement, la cybersécurité devrait être prise en compte dès le début.

Le Conseil Supérieur préconise donc que les autorités encouragent et soutiennent des projets au sein des secteurs professionnels dans le cadre desquels on travaille concrètement sur la digitalisation et la cybersécurité de la profession.

9. La cybersécurité est une mission publique fondamentale

La sécurité physique est généralement considérée comme un droit fondamental et son assurance comme une mission publique fondamentale. Toutefois, la cybersécurité est souvent considérée comme la responsabilité de l'entreprise ou comme une responsabilité partagée. L'accent mis sur la responsabilité de l'entreprise dans le cadre du Règlement général sur la protection des données a contribué à ce phénomène. Le Conseil Supérieur reconnait que les PME doivent assumer une responsabilité et un rôle dans le cadre de leur protection contre la cybercriminalité. En effet, le Conseil Supérieur et ses membres mènent des actions visant à sensibiliser et aider les PME dans ce domaine. Il n'en demeure pas moins que l'assurance de la cybersécurité est une mission publique fondamentale et que les PME doivent avant tout être considérées comme des victimes (potentielles).

Par conséquent, le Conseil Supérieur demande aux autorités de faire tout ce qui est en leur pouvoir afin de renforcer la cybersécurité des PME, d'une part en luttant contre la cybercriminalité et d'autre part en contribuant à l'amélioration de la cyberprotection des PME. Pour ces raisons, le Conseil Supérieur estime inacceptable que la *Federal Computer Crime Unit* (FCCU) de la Police Fédérale soit confrontée à un manque de personnel. Ce service devrait être une des priorités de la politique gouvernementale de lutte contre la cybercriminalité. La justice devrait également faire de la cybercriminalité une priorité. Dans le cadre de la collaboration internationale et de la diplomatie, il conviendrait de viser à ce que les États tiers entreprennent les actions nécessaires afin d'identifier et de pénaliser les cybercriminels. Quant au Centre pour la Cybersécurité Belgique (CCB) et à l'équipe *Computer Emergency Response Team* (CERT) qui en fait partie, le Conseil Supérieur préconise que ces services soient fortement élargis, afin que toutes les entreprises puissent bénéficier de leur assistance et pas seulement les entreprises fournissant des services critiques.

10. Nécessité d'harmoniser les politiques

La cybersécurité implique de nombreux acteurs et niveaux politiques. Pour les PME, il importe toutefois peu qui fait quoi, du moment que ce soit réalisé et réalisé de manière convenable. L'implication des différents niveaux de pouvoir et acteurs politiques est également positive, vu qu'elle permet de mobiliser de nombreuses ressources. Un niveau minimum d'harmonisation et de coopération est toutefois nécessaire pour y parvenir. Si les différents niveaux de pouvoir, Ministres et administrations mènent leurs politiques en partant de leurs propres compétences et sans harmonisation, des problèmes tels que des chevauchements, de la fragmentation, des oppositions, une intégration réduite de la politique par le groupe cible, des hiatus et des synergies perdues se poseront. Les PME ont besoin d'informations claires, simples et sans équivoque. En effet, elles éprouvent davantage de difficultés quand elles se voient offrir des informations et un soutien similaires de plusieurs côtés. En même temps, certaines actions utiles ne sont entreprises par aucune autorité. En collaborant entre elles, les autorités pourraient également renforcer leurs actions respectives. Une bonne harmonisation dans toutes les phases du cycle politique et entre tous les acteurs concernés est donc indispensable.

Pourtant, le Conseil Supérieur constate qu'à l'heure actuelle, il y a très peu de coordination:
- Actuellement, l'harmonisation stratégique/politique est pratiquement inexistante.
- Différents acteurs élaborent des scans de cybersécurité et outils d'évaluation similaires.

- Il existe plusieurs brochures et guides informatifs qui ne sont pas ou peu alignés entre eux.
- Les différentes autorités ne sont pas au courant des campagnes d'information menées par leurs pairs.
- Les PME doivent signaler les cyberincidents auprès de plusieurs instances.
- …

Par conséquent, le Conseil Supérieur incite tous les acteurs à miser davantage sur l'harmonisation systématique, en utilisant les structures existantes ou en créant, si nécessaire, de nouvelles structures à cette fin.

11. Promouvoir la collaboration

La cybersécurité implique de nombreux acteurs. Incontestablement, la collaboration entre ces différents acteurs conduira à de meilleurs résultats. Les PME peuvent collaborer entre elles via leurs organisations professionnelles et interprofessionnelles. À leur tour, les organisations d'entrepreneurs peuvent également coopérer entre elles. En outre, de nombreux partenariats et synergies avec d'autres acteurs publics et privés sont possibles.

Quand il s'agit par exemple de mettre des informations et outils à la disposition des PME, il pourrait être envisagé de collaborer non seulement avec les organisation d'entrepreneurs et les acteurs publics, mais également avec d'autres acteurs qui constituent un bon moyen d'interaction avec les PME et qui bénéficient de leur confiance. Presque toutes les PME font appel à un opérateur télécom, à une institution financière, à une compagnie d'assurance et souvent aussi à un comptable et à un prestataire de services TIC. Le rôle spécifique des opérateurs télécom leur permet également de fournir plus de solutions technologiques aux PME. Quant aux prestataires de services TIC, il conviendrait de prendre des initiatives visant à offrir à ce groupe une formation plus détaillée en matière de cybersécurité. Ainsi, la cybersécurité des nombreuses PME faisant appel à un soutien TIC externe pourrait être améliorée et le problème de la pénurie de talents dans le domaine de la cybersécurité pourrait être partiellement appréhendé.

De nombreux projets intéressants bénéficiant à la cybersécurité des PME (tels que la création d'une plateforme proposant des tests de phishing pour les PME, l'évaluation des risques de cybersécurité par secteur professionnel, l'évaluation des solutions cloud pour les PME du point de vue de la cybersécurité, ...) pourraient être réalisés par le biais d'une coopération entre les centres d'expertise, les organisations des entrepreneurs et les autorités.

Par conséquent, le Conseil Supérieur invite les responsables politiques à promouvoir et soutenir les formes de collaboration décrites ci-dessous. Ainsi, le rôle du Conseil Supérieur dans le domaine de la cybersécurité pourrait être renforcé en prévoyant un financement spécifique afin qu'il puisse consacrer davantage de temps à ce sujet.

CONCLUSION

La cybercriminalité constitue une menace croissante pour les PME. Dès lors, la cybersécurité des PME constitue une priorité politique essentielle sur laquelle il convient de miser davantage. Dans le présent avis, le Conseil Supérieur a exposé sa vision sur la cybersécurité des PME ainsi que sur la politique gouvernementale en la matière. Il a défini les lignes directrices dont, selon lui, la politique devrait tenir compte et les a reliées à des propositions d'action. La tableau ci-dessous résume ces lignes directrices et actions.

1. Un problème réel
- Informer et sensibiliser les PME de manière permanente sur le risque encouru - Construire une campagne autour de témoignages des PME victimes de cybercriminalité - Accroître la volonté des PME de signaler les incidents - Une meilleure collecte de données en matière de cyberincidents + typologie commune
2. La grande majorité des entreprises sont des petites entreprises
- Les PME comme point de référence et norme - Prévoir un nombre suffisant d'initiatives visant spécifiquement les PME - Ne pas oublier que la plupart des PME ne sont pas des entreprises numériques ou de haute technologie - Segmenter encore davantage le groupe des PME
3. Situation spécifique des PME
- Une attention suffisante et spécifique pour les PME
4. Sensibilisation et formation à la mesure des PME
- Une approche pragmatique mettant l'accent sur la prévention, la sensibilisation, la formation et un changement de comportement concret - Des informations et outils concrets et pratiques à la mesure des PME - Regrouper les informations et outils pour les PME sur un seul site web - Pour des actions nécessitant une expertise spécifique, prévoir des aides publiques + une check-list prestataire de services - Approche prudente de la certification des PME. La certification des logiciels et des services TIC serait une bonne piste.
5. Miser sur des solutions technologiques
- Renforcer l'offre de solutions technologiques, les rendre appropriées et accessibles et stimuler leur utilisation - Veiller à ce que les PME n'utilisent que des logiciels sécurisés
6. Évaluation des risques pour une protection adaptée
- Soutenir les évaluations sectorielles des risques - Veiller à ce que davantage de données fiables soient collectées sur les cybermenaces pesant sur les PME belges - Analyser l'efficience et l'efficacité des actions et mesures, tant au niveau des PME qu'au niveau politique - Comparer l'approche des autres pays - Considérer le rôle des cyberassurances
7. Une approche spécifique à la profession ou au secteur
- Dans la mesure du possible, adopter une approche axée sur la spécificité des professions ou secteurs - Encourager et stimuler des initiatives spécifiques à la profession ou au secteur
8. La cybersécurité en tant que partie de la digitalisation
- Encourager et soutenir des projets sur la digitalisation et la cybersécurité au sein des secteurs professionnels

9. La cybersécurité est une mission publique fondamentale
- Lutter contre la cybercriminalité et contribuer à l'amélioration de la cyberprotection - Renforcer le rôle de la FCCU, de la justice, de la collaboration internationale et de la diplomatie - Renforcer CCB/CERT afin que toutes les PME puissent bénéficier de leur assistance en cas d'incidents
10. Nécessité d'harmoniser les politiques
- Davantage d'harmonisation systématique, via les structures existantes ou, si nécessaire, via de nouvelles structures
11. Promouvoir la collaboration
- Travailler avec des partenaires de confiance ayant accès aux PME - Initiatives visant à former les prestataires de services TIC de manière plus détaillée en matière de cybersécurité - Encourager et soutenir la coopération entre les centres d'expertise, les organisations des entrepreneurs et les autorités - Renforcer le rôle du CSIPME en matière de cybersécurité