F Stratégie cyberséc A1 **Bruxelles, le 24 septembre 2024**
MH/JC/JP
940-2024

AVIS

sur

LA PRÉPARATION DE LA STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2026-2030

Conseil Supérieur des Indépendants et des PME
City Atrium C (4ème étage) - Rue du Progrès 50 - 1210 Bruxelles
Tél. : 02 277 90 16 - secr@hrzkmo-csipme.fgov.be - www.csipme.fgov.be

Le Centre pour la Cybersécurité Belgique (CCB) a sollicité l'avis du Conseil Supérieur des Indépendants et des PME en préparation de la nouvelle stratégie nationale de cybersécurité pour la période 2026-2030. Après consultation du groupe de travail permanent Digitalisation, Cybersécurité et RGPD, le Bureau du Conseil Supérieur a émis en urgence le 24 septembre 2024 l'avis suivant.

CONTEXTE

Le Centre pour la Cybersécurité Belgique (CCB) a demandé la contribution du Conseil Supérieur pour une nouvelle stratégie nationale de Cybersécurité couvrant la période 2026-2030. La stratégie nationale actuelle, à savoir la Stratégie nationale de Cybersécurité 2.0[1], a été approuvée par le Conseil national de sécurité en 2021 et couvre la période 2021-2025. Cette période prenant fin l'année prochaine et la nouvelle directive européenne NIS-2 imposant en outre de nouvelles obligations auxquelles les stratégies nationales de cybersécurité devront se conformer, une nouvelle stratégie belge de cybersécurité révisée s'impose. Le CCB est responsable, en tant qu'autorité nationale, de l'élaboration de cette stratégie. Dans sa demande d'avis, le CCB souligne que l'approche actuelle consiste à diviser le domaine cyber en quatre sous-domaines politiques : Cybersécurité (Prévention-Protection-Réaction), Lutte contre la cybercriminalité, Cyberdéfense et Cyberdiplomatie. Le CCB travaille uniquement sur une stratégie spécifique pour le domaine de la cybersécurité. Dans sa demande d'avis, il indique également qu'il souhaite mettre l'accent sur l'offre des services dans la prochaine stratégie. Dès lors, le CCB sollicite l'avis, les suggestions et les contributions générales du Conseil Supérieur concernant les objectifs et services qui peuvent être inclus dans la prochaine stratégie de cybersécurité.

La cybersécurité n'est pas un thème nouveau pour le Conseil Supérieur. En effet, le Conseil Supérieur et les organisations professionnelles et interprofessionnelles agréées représentées en son sein contribuent également à l'amélioration de la cybersécurité des PME. En interne, le Conseil Supérieur réunit ses membres sur ce sujet au sein d'un groupe de travail permanent Digitalisation, Cybersécurité et RGPD. Depuis 2018, il 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. De plus, le Conseil Supérieur collabore étroitement avec le CCB et le SPF Economie afin d'améliorer la cybersécurité des PME. Il fait partie du *National Cybersecurity Council Belgium* (NCCB) du CCB. Au niveau du SPF Economie, il est étroitement associé à la préparation et la mise en œuvre du programme Cyber4SME. En particulier, le Conseil Supérieur souhaite ici attirer l'attention sur son avis de 2021 sur la politique gouvernementale relative à la cybersécurité des PME[2]. Dans ledit avis, il a formulé les principes, lignes directrices et points d'attention dont, selon lui, la politique devrait tenir compte et il les a reliés à un certain nombre de propositions d'action concrètes. Presque tous les points de vue exprimés dans cet avis sont toujours d'actualité. Certains d'entre eux seront brièvement rappelés dans le présent avis.

[1] Disponible en ligne via ce lien.
[2] Avis n° 845 du CSIPME du 16 février 2021 (entériné par l'Assemblée plénière le 6 mai 2021) sur la politique gouvernementale relative à la cybersécurité des PME (disponible en ligne via ce lien).

POINTS DE VUE

1. Il est bon d'impliquer les parties prenantes

Le Conseil Supérieur se félicite du fait que le CCB implique les parties prenantes et demande leurs contributions à un stade précoce dans le cadre de l'élaboration de la stratégie nationale de cybersécurité. Cette démarche contribuera à une meilleure stratégie et renforcera également le soutien apporté à celle-ci et à sa mise en œuvre.

Il conviendrait également que cette étroite collaboration avec les différentes parties prenantes, et notamment avec celles qui représentent les PME, soit explicitement inscrite dans la nouvelle stratégie. En effet, une stratégie de cybersécurité ne sera couronnée de succès que si tous les acteurs concernés collaborent. Cela s'inscrit également dans le prolongement de la vision et de la manière de fonctionner actuelles du CCB.

Le Conseil Supérieur préconise que le projet de stratégie soit également soumis pour avis.

2. Considérer les PME et leur spécificité

Au cours des dernières années, tous les acteurs concernés ont déployé des efforts considérables afin d'augmenter la cybersécurité des PME. Ces travaux ont eu un impact. Davantage de PME sont conscientes des cyber-risques et ont pris certaines mesures. En général, la sensibilisation et la cyberrésilience des PME restent toutefois très faibles. En outre, les cybermenaces et les cyber-risques ont augmenté.[3] Le renforcement de la cybersécurité des PME reste donc un défi toujours aussi important. De plus, il convient de noter que la Belgique compte quelques 1.144.000 entreprises, dont environ 1.136.000 (soit 99,3%) sont des PME (< 50 salariés)[4]. Ces PME constituent l'épine dorsale de notre économie. Le Conseil Supérieur estime qu'il conviendrait donc de leur accorder une attention particulière dans le cadre de la nouvelle stratégie nationale de cybersécurité.

En outre, il convient de tenir compte de la spécificité des PME. En effet, 99,3% des entreprises belges sont des PME, mais 96,7% des entreprises belges sont des micro-entreprises (< 10 salariés) et 83% d'entre elles n'occupent pas de personnel. Les PME, et en particulier les micro-entreprises et les entreprises individuelles, fonctionnent d'une manière tout à fait différente des grandes entreprises. Ainsi, elles ne disposent souvent pas de leur propre service TIC et sont confrontées à un certain nombre d'inconvénients d'échelle. Par conséquent, le Conseil Supérieur plaide pour une politique et pour des informations et des mesures de soutien à la mesure des PME.

En outre, le fait d'accorder une attention particulière aux PME profite non seulement à ces dernières, mais également à l'ensemble de la chaîne d'approvisionnement. Les PME, en particulier celles qui ne disposent pas de leur propre service TIC, courent un risque plus élevé d'être victimes d'une cyberattaque et peuvent ainsi, sans le vouloir, constituer un danger pour les autres entreprises (plus grandes) de la chaîne d'approvisionnement dont elles font partie. Par conséquent, si les autorités apportent un soutien supplémentaire à ces PME, toutes les entreprises en bénéficieront.

---

[3] Voir entre autres le *CS-barometer* (baromètre CS) le plus récent du EWI (note de la traductrice : Département Economie, Sciences et Innovation des autorités flamandes), ainsi que le rapport *Digitale fitheid 2024* (Aptitude numérique 2024) d'Unizo.

[4] Source: Statbel - SPF Economie, PME, Classes moyennes et Energie. Situation au 31/12/2022.

3. Mesures de prévention et de protection

Le Conseil Supérieur estime qu'en ce qui concerne les PME, il convient d'opter pour des mesures de protection. Dans sa demande d'avis, le CCB fait une distinction entre la prévention, la protection et la réaction. Pour le Conseil Supérieur, la distinction entre la prévention et la protection n'apparait pas clairement dans ce cas. En règle générale, le Conseil Supérieur lui-même se base sur les six domaines du *NIST Cybersecurity Framework 2.0: identify, protect, detect, respond, recover* et *govern*. Si tous les domaines requièrent une attention adéquate, il est préférable pour les PME de se concentrer en priorité sur des actions qui favorisent la protection. De telles actions ont également par définition un effet préventif. La plupart du temps, l'impact d'un cyber-incident sur une PME est tellement grave que les actions préventives sont à privilégier.

Ces actions devraient viser à la fois les éléments humains, technologiques et de processus de la cybersécurité. En effet, de nombreux cyber-incidents résultent d'erreurs ou de choix humains. Toutefois, les PME peuvent diminuer ce facteur humain et améliorer sensiblement leur cybersécurité de manière relativement simple, par exemple par le biais de formations en matière de cyber-hygiène élémentaire. La technologie et les processus jouent également un rôle important. Une PME devra donc être attentive à ces trois types d'actions.

Le Conseil Supérieur préconise également de continuer à investir dans des stratégies et des technologies qui protègent les entrepreneurs sans que ceux-ci aient à faire quoi que ce soit ou à s'en préoccuper eux-mêmes. Dès lors, il soutient des projets CCB tels que le *Belgian Anti-Phishing Shield, stop smishing* et *spear warning*. Il reste également nécessaire de poursuivre les efforts de sensibilisation et de formation des PME et de leur personnel. Toutefois, il est encore mieux de pouvoir éliminer une menace avant qu'elle n'atteigne les PME ou de pouvoir informer ces dernières de manière très ciblée sur des menaces spécifiques.

Le Conseil Supérieur souhaite également souligner l'importance de garantir la cybersécurité des logiciels utilisés par les PME. Les PME doivent pouvoir se fier aux logiciels qu'elles utilisent, surtout si elles les mettent à la disposition de leurs propres clients.

En ce qui concerne les mesures à adopter, le Conseil Supérieur est donc évidemment favorable à la stratégie de Cyberprotection active (ACP)[5] du CCB, qui représente une approche proactive, sur mesure, automatisée et participative.

4. Comment atteindre les PME?

Les PME sont très nombreuses et, bien qu'elles ne comptent généralement qu'une ou quelques personnes, elles sont inondées d'informations sur des sujets très variés. C'est pourquoi il est très difficile d'atteindre les PME ou de les inciter à l'action. Une des questions clés est donc de savoir quels sont les canaux de communication les plus adaptés.

Le Conseil Supérieur est convaincu que les organisations de PME en particulier constituent un excellent canal. En effet, elles connaissent leurs membres, jouissent de leur confiance et disposent des canaux de communication nécessaires. Dans le cas des organisations professionnelles, leurs membres sont en outre souvent confrontés à des défis fort similaires en

[5] https://ccb.belgium.be/sites/default/files/documents/ACP_Policy_Document_FR.pdf

matière de TIC et de cybersécurité. Ainsi, les organisations professionnelles sont les partenaires les mieux placés pour informer les PME et les aider à renforcer leur cyberrésilience. Il convient que les autorités soutiennent activement les organisations de PME à cette fin.

En deuxième lieu, le Conseil Supérieur songe également au prestataires de services TIC. En effet, de nombreuses PME font appel à des prestataires de services TIC. Par conséquent, ces derniers sont les partenaires de choix pour aider les PME à améliorer leur cybersécurité. Toutefois, ces prestataires de services TIC ne disposant pas non plus tous des connaissances et des compétences nécessaires à cette fin, le Conseil Supérieur préconise que des projets soient développées afin de les aider à assumer ce rôle.

En outre, presque toutes les PME ont aussi leur opérateur de télécommunication, leur banque, leur assureur et souvent aussi leur expert-comptable. Ces canaux permettent également d'atteindre les PME.

Enfin, le Conseil Supérieur estime qu'il convient également d'informer et de soutenir les petites entreprises au niveau local. Par le biais des associations d'entreprises locales, des services de sécurité intégrale des villes et des communes et des zones de police locale, il est possible d'atteindre des entrepreneurs qui sont difficilement joignables par les autres canaux. Par exemple, tout comme de nombreuses villes et communes proposent déjà des conseils en matière de prévention des cambriolages, des conseils en matière de cybersécurité devraient également être offerts aux petits entrepreneurs. Le Conseil Supérieur émettra un avis distinct à ce sujet et soutient également un projet pilote en la matière.

5. La cybersécurité comme partie de la digitalisation

Pour de nombreuses PME, une digitalisation plus poussée représente également un défi. Au lieu d'aborder la digitalisation et la cybersécurité comme deux défis différents, il conviendrait de miser sur une digitalisation en toute cybersécurité: Comment une PME peut-elle s'organiser au mieux sur le plan digital? Et comment le faire en toute cybersécurité? Il s'agit là d'une approche logique 'by design' de la cybersécurité. De plus, une telle approche motivera davantage les PME à agir, les avantages qu'elles tireront d'une digitalisation plus poussée étant plus visibles. Etant donné que les PME actives au sein d'un même secteur sont confrontées à des défis numériques similaires, il serait préférable que les autorités les soutiennent dans ce cadre par l'intermédiaire des organisations professionnelles.

6. Compétences numériques du personnel et des clients

Les entrepreneurs de PME doivent renforcer leurs compétences numériques, mais la cybersécurité des PME dépend également de plusieurs autres groupes tels que le personnel, les clients et les prestataires de services TIC. Par conséquent, il conviendrait que toutes les formes d'enseignement et de formation accordent une plus grande attention aux compétences numériques, y compris à la cybersécurité. Si le client d'une PME est victime d'une cyberfraude, cela rejaillit ou peut également avoir des répercussions sur la PME concernée. Le citoyen/client est souvent le maillon le plus faible et le Conseil Supérieur est donc évidemment favorable à ce que le gouvernement déploie encore plus d'efforts pour informer et soutenir le citoyen.

7. Un helpdesk cybersécurité pour les PME

Le Conseil Supérieur demande que la fonction CERT du CCB[6] soit étendue à toutes les entreprises. Toutes les PME devraient pouvoir s'adresser au CCB pour obtenir des conseils de première ligne en cas de cyber-incident.

Dans de nombreux cas, les organisations de PME sont également un premier point de contact pour les entrepreneurs lorsque ceux-ci sont confrontés à des questions ou à des problèmes. A cette fin, certaines organisations de PME ont créé leurs propres centres d'appel. Par cette voie, elles reçoivent donc également de nombreuses questions et rapports relatifs à des cyber-incidents. Il importe qu'elles puissent les transmettre au CCB de manière systématique et qu'une coopération soit mise en place à cette fin.

8. Tenir compte des PME dans le cadre de la certification

Le Conseil Supérieur reconnaît l'utilité que peuvent avoir les certificats et les labels dans le domaine de la cybersécurité. Or, en raison de leur échelle plus réduite, il est plus difficile pour les PME que pour les grandes entreprises d'obtenir de tels certificats ou labels. C'est pourquoi le Conseil Supérieur s'oppose résolument à ce que les PME soient soumises à des obligations en matière de certificats ou de labels. Il convient avant tout d'encourager et de soutenir les PME afin d'améliorer leur cybersécurité. Dans ce cadre, des labels ou certificats peuvent, en tant qu'instrument volontaire, être utiles aux PME.

Dans les cas où des certificats ou des labels sont nécessaires et obligatoires (par exemple si l'on entre dans le champ d'application de la directive NIS-2), le Conseil Supérieur plaide pour des instruments adaptés aux et réalisables pour les PME.

Les certificats et labels peuvent également apporter une solution à l'effet de ruissellement, c'est-à-dire lorsque les grandes entreprises imposent, en raison de leurs propres obligations, des obligations de rapportage (divergentes) aux PME avec lesquelles elles collaborent ou leur demandent des certificats (difficiles à obtenir). Dans de tels cas, une norme simple et uniforme pour les PME pourrait constituer une solution et simplifier la situation tant pour les PME que pour les grandes entreprises.

Pour ces différentes raisons, le Conseil Supérieur soutient et promeut l'initiative CyberFundamentals Framework[7] du CCB. Ce cadre a l'avantage de prévoir des labels dûment étayés à différents niveaux (*Small, Basic, Important* et *Essential*), de sorte que les PME puissent également les utiliser.

Comme mentionné ci-dessus, il est en outre très important pour les PME de pouvoir se fier aux logiciels qu'elles utilisent et aux services TIC qu'elles achètent. Dans ce contexte également, des certificats et labels ou d'autres systèmes d'assurance qualité pourraient constituer une solution.

[6] Cyber Emergency Response Team (https://ccb.belgium.be/fr/cert)
[7] https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework

9. Evaluer l'impact des mesures

Le Conseil Supérieur est partisan d'une évaluation ex ante et ex post des mesures politiques. Or, lorsqu'il s'agit de mesures visant à renforcer la cybersécurité des PME, il est important de considérer l'impact réel. L'expérience a montré qu'il est très difficile de convaincre les PME de participer à des initiatives visant à améliorer leur cybersécurité. Par conséquent, plusieurs projets ne touchent qu'un nombre limité de PME. Toutefois, en mesurant l'impact d'un projet, il convient de ne pas se limiter à considérer le nombre de PME atteintes. En effet, les cyber-incidents peuvent avoir un impact très important pour une PME et entraîner des coûts très élevés. Par conséquent, il convient de mesurer l'impact des mesures politiques en termes de dommages évités.

10. Coordination entre les acteurs publics

La cybersécurité implique de nombreux acteurs et niveaux politiques. Cette implication est positive, vu qu'elle permet de mobiliser de nombreuses ressources. En revanche, la nécessité d'une meilleure harmonisation et d'une approche stratégique et opérationnelle plus uniforme est évidente.

Les PME requièrent des informations et un soutien 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. A l'heure actuelle, les PME peuvent trouver des informations et des mesures de soutien des pouvoirs publics à la fois auprès du CCB, du SPF Économie et des organisations régionales VLAIO, AdN et hub.brussels. Il serait préférable de regrouper ces informations et ce soutien sur un site web unique. A tout le moins, il conviendrait qu'un aperçu de toutes les mesures soit fourni quelque part et que les différents sites web et initiatives renvoient à cet aperçu ou l'un à l'autre. Une bonne harmonisation dans toutes les phases du cycle politique et entre tous les acteurs concernés est indispensable.

11. Statistiques communes

On manque encore nettement de données sur les cyber-risques et -incidents. Pourtant, ces données sont importantes pour les entreprises et les secteurs d'activité, afin de leur permettre de prendre des décisions réfléchies. De même, les autorités ne peuvent mener des politiques efficaces et effectives que si elles disposent de données suffisantes en appui de ces politiques. Les informations existantes sont dispersées et basées sur des méthodologies et des typologies différentes. Le Conseil Supérieur préconise qu'un groupe de travail soit mis en place au sein du CCB ou de la Cyber Security Coalition avec pour objectif d'améliorer la disponibilité des données relatives aux cyber-risques et -incidents. Ce groupe de travail pourrait réunir tous les partenaires publics et privés concernés, identifier les données disponibles et les lacunes, développer conjointement des méthodologies et des typologies, etc.

12. Recherches multidisciplinaires

Il est important que la Belgique investisse dans la recherche en matière de cybersécurité. La combinaison de la cybersécurité et de l'IA en particulier semble être un fer de lance intéressant pour la recherche. En outre, le Conseil Supérieur estime qu'il est intéressant d'investir non seulement dans la recherche technologique, mais également dans les recherches qui

s'intéressent à des aspects moins techniques tels que la sensibilisation, la spécificité des PME, les données issues des sciences comportementales, le coût de la cybercriminalité pour les entreprises, etc. De la même manière que les entreprises devraient aborder la cybersécurité pas uniquement sous l'angle des TIC mais également de manière multidisciplinaire, une approche multidisciplinaire devrait également être adoptée dans le cadre de la recherche par les universités et les écoles supérieures.

13. Cyberassurances

Le Conseil Supérieur ne considère pas les cyberassurances comme des solutions isolées, mais plutôt comme ultime complément à une série de mesures de cybersécurité prises par une organisation ou un citoyen. Le marché de la cyberassurance évolue vite. Il convient que les autorités surveillent ce marché en collaboration avec les acteurs concernées. Par ailleurs, il conviendrait également d'examiner si dans certains cas d'autres mécanismes de solidarité, tels qu'un fonds d'urgence, ne pourraient pas être mis en place. Dans ce cadre, le Conseil Supérieur demande également de veiller à ce que tous les acteurs assument leurs responsabilités. Par exemple, de nombreuses indications montrent qu'en cas de fraude bancaire, les banques rejettent trop facilement la faute sur leurs clients PME et ne veulent pas réparer le préjudice.

CONCLUSION

Le Conseil Supérieur demande que les PME, qui constituent l'épine dorsale de notre économie, fassent l'objet d'une attention particulière dans le cadre de la nouvelle stratégie nationale de cybersécurité. En règle générale, la cybersécurité des PME est très faible, alors que les cybermenaces et cyber-risques ne font qu'augmenter. Dans ce cadre, il convient également de tenir compte de la spécificité des PME. En effet, elles ont besoin d'informations et de mesures de soutien à leur mesure. C'est dans cette optique que le Conseil Supérieur formule, dans le présent avis, une série de points de vue relatifs aux objectifs et aux services du CCB. Il demande qu'il en soit tenu compte lors de l'élaboration de la stratégie nationale.