Parlement européen
2019-2024

Commission de l'industrie, de la recherche et de l'énergie

2023/0108(COD)

21.9.2023

AMENDEMENTS
17 - 52

Projet de rapport
Josianne Cutajar
(PE752.802v01-00)

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement(UE) 2019/881 en ce qui concerne les services de sécurité gérés

Proposition de règlement
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Amendement 17
Evžen Tošenovský

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) Les services de sécurité gérés, ***qui*** consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, ont gagné en importance en ce qui concerne la prévention et de la limitation des incidents de cybersécurité. En conséquence, les fournisseurs de ***tels*** services sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555 ***du Parlement européen et du Conseil***[8]. Au titre du considérant 86 de ladite directive, les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.	(2) Les services de sécurité gérés ***sont des services fournis par les fournisseurs de services de sécurité gérés conformément à l'article 6***, ***point 40), de la directive (UE) 2022/2555 du Parlement européen et du Conseil. Ces services*** consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, ***et*** ont gagné en importance en ce qui concerne la prévention et de la limitation des incidents de cybersécurité. En conséquence, les fournisseurs de services ***de sécurité gérés*** sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de ***l'annexe I, point 10), de*** la directive (UE) 2022/2555. Au titre du considérant 86 de ladite directive, les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.
_____	_____

[8] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

[8] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

Or. en

Amendement 18
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) Les services de sécurité gérés, qui consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, ont gagné en importance en ce qui concerne la prévention et ***de*** la limitation des incidents de cybersécurité. En conséquence, les fournisseurs de tels services sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[8] . Au titre du considérant 86 de ladite directive, les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et, du fait	(2) Les services de sécurité gérés, qui consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, ***notamment en ce qui concerne la prévention ou la détection des incidents ainsi que la réponse apportée et le rétablissement à la suite de ceux-ci,*** ont gagné en importance en ce qui concerne la prévention et la limitation des incidents de cybersécurité. En conséquence, les fournisseurs de tels services sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[8]. Au titre du considérant 86 de ladite directive, les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se

de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

[8] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

[8] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

Or. en

Amendement 19
Evžen Tošenovský

Proposition de règlement
Considérant 3

Texte proposé par la Commission	*Amendement*
(3) Les fournisseurs de services de sécurité gérés jouent également un rôle important concernant la réserve de cybersécurité de l'UE, dont la mise en place progressive est soutenue par le règlement (UE).../.... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir]. La réserve de cybersécurité de l'UE doit être utilisée pour soutenir les mesures de réaction et de rétablissement	(3) Les fournisseurs de services de sécurité gérés jouent également un rôle important concernant la réserve de cybersécurité de l'UE, dont la mise en place progressive est soutenue par le règlement (UE).../.... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir]. La réserve de cybersécurité de l'UE doit être utilisée pour soutenir les mesures de réaction et de rétablissement

immédiat en cas d'incidents de cybersécurité importants et de grande ampleur. Le règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir] met en place un processus de sélection des fournisseurs constituant la réserve de cybersécurité de l'UE, qui devrait, entre autres, tenir compte du fait que le fournisseur concerné a obtenu une certification européenne ou nationale en matière de cybersécurité. ***Les services pertinents fournis par des «fournisseurs*** de ***confiance» au titre du règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et*** les ***capacités dans l'Union afin*** de ***détecter les menaces et incidents*** de ***cybersécurité,*** de ***s'y préparer et d'y réagir] correspondent aux «services*** de sécurité ***gérés» conformément au présent règlement***.

immédiat en cas d'incidents de cybersécurité importants et de grande ampleur. Le règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir] met en place un processus de sélection des fournisseurs ***de services de sécurité gérés de confiance*** constituant la réserve de cybersécurité de l'UE, qui devrait, entre autres, tenir compte du fait que le fournisseur concerné a obtenu une certification européenne ou nationale en matière de cybersécurité. ***En outre, une fois qu'un schéma européen de certification*** de ***cybersécurité pour les services de sécurité gérés sera en place, lequel schéma remplacerait également tous*** les ***schémas nationaux de certification*** de ***cybersécurité pertinents, une certification obligatoire au titre*** de ***ce schéma*** de ***certification devrait s'appliquer en vue de l'ajout de fournisseurs de services*** de sécurité ***gérés de confiance à la réserve de cybersécurité de l'UE***.

Or. en

Amendement 20
Johan Nissinen

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) La certification des services de sécurité gérés est non seulement pertinente dans le processus de sélection de la réserve de cybersécurité de l'UE, mais elle constitue également un indicateur de qualité essentiel pour les entités privées et publiques qui ont l'intention d'acheter de tels services. Compte tenu de la criticité des services de sécurité gérés et du	(4) La certification des services de sécurité gérés est non seulement pertinente dans le processus de sélection de la réserve de cybersécurité de l'UE, mais elle constitue également un indicateur de qualité essentiel pour les entités privées et publiques qui ont l'intention d'acheter de tels services. Compte tenu de la criticité des services de sécurité gérés et du

caractère sensible des données qu'ils traitent, la certification pourrait fournir aux clients potentiels des orientations et une assurance importantes quant à la fiabilité de ces services. Les schémas européens de certification pour les services de sécurité gérés contribuent à éviter la fragmentation du marché unique. Le présent règlement vise donc à améliorer le fonctionnement du marché intérieur.

caractère sensible des données qu'ils traitent, la certification pourrait fournir aux clients potentiels des orientations et une assurance importantes quant à la fiabilité de ces services. Les schémas européens de certification pour les services de sécurité gérés contribuent à éviter la fragmentation du marché unique. Le présent règlement vise donc à améliorer le fonctionnement du marché intérieur. ***Dans le même temps, il convient de trouver un équilibre entre les multiples objectifs du règlement, d'une part, et la charge réglementaire et les coûts potentiels liés à la certification, d'autre part, étant donné que le respect des exigences en matière de certification entraînera des dépenses et des efforts administratifs supplémentaires, ce qui pourrait constituer un problème pour les petits prestataires.***

Or. en

Amendement 21
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Considérant 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(4 bis) Le marché et les systèmes éducatifs offrant une multitude de ressources pédagogiques et de formations formelles, il convient de souligner qu'il est également possible d'acquérir des connaissances de manière informelle et que les compétences peuvent être démontrées au moyen de diplômes et de certifications, mais pas uniquement. En particulier dans le contexte actuel, où les menaces évoluent rapidement, les États membres et les bénéficiaires de services de sécurité gérés devraient tenir compte des chercheurs hautement qualifiés qui recherchent les vulnérabilités. En outre,

les entités et personnes physiques qui recherchent les vulnérabilités peuvent, dans certains États membres, être exposées à la responsabilité pénale et civile, c'est pourquoi les États membres sont encouragés à publier des lignes directrices concernant l'absence de poursuites contre les auteurs de recherches en matière de sécurité de l'information et une exemption de responsabilité civile pour ces activités.

Or. en

Justification

L'environnement dans lequel évoluent les professionnels de la sécurité varie en partie en raison du fait que leurs parcours professionnels, leur accès à l'éducation formelle et les ressources leur permettant d'obtenir une certification ne sont pas standardisés. Par conséquent, nous devons encourager l'emploi de personnes qualifiées et garantir un cadre positif pour les activités qui mènent à une amélioration de la cybersécurité.

Amendement 22
Josianne Cutajar

Proposition de règlement
Considérant 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(4 bis) Le schéma de certification de l'Union pour les services de sécurité gérés devrait garantir la disponibilité de services sûrs et de haute qualité qui garantissent une transition numérique sûre et contribuent à la réalisation des objectifs fixés dans le programme d'action «La voie à suivre pour la décennie numérique[8 bis]», en particulier en ce qui concerne l'objectif consistant à ce que 75 % des entreprises de l'Union commencent à utiliser l'informatique en nuage, l'IA ou les mégadonnées, à ce que plus de 90 % des PME atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient proposés en ligne.

[8 bis] ***Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030.***

Or. en

Amendement 23
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(4 bis) Les schémas européens de certification des services de sécurité gérés devraient faciliter le recours à ces services, en particulier pour les entités plus petites, notamment les collectivités locales et régionales ou les PME, qui ne disposent souvent pas des capacités financières et humaines nécessaires pour assurer ces services par elles-mêmes mais qui sont vulnérables aux cyberattaques susceptibles d'avoir des conséquences importantes.

Or. en

Amendement 24
Josianne Cutajar

Proposition de règlement
Considérant 5

Texte proposé par la Commission	*Amendement*
(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent	(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent

en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA],

en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Le ***schéma de certification établi en vertu du présent règlement devrait également tenir compte des résultats et des recommandations de l'évaluation et de la révision prévues à l'article 67 dudit règlement. Le*** Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA],

Or. en

Amendement 25
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 5

Texte proposé par la Commission	*Amendement*
(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité des services	(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité ***et la fiabilité***

de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA],	des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA],

Or. en

Amendement 26
Evžen Tošenovský

Proposition de règlement
Considérant 5

Texte proposé par la Commission	*Amendement*
(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Le Contrôleur européen de la	(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification ***spécifique***, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. Le Contrôleur

protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA],	européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA],

Or. en

Amendement 27
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 bis) Étant donné que les schémas européens de cybersécurité devraient certifier que les services de sécurité gérés sont fournis par un personnel hautement qualifié capable de fournir ces services de manière fiable et de garantir les normes de cybersécurité les plus élevées, il est impératif que l'Union dispose de suffisamment de personnel hautement qualifié. Toutefois, l'Union est confrontée à une pénurie de talents, caractérisée par un manque de professionnels qualifiés et par l'évolution rapide des menaces, comme l'a reconnu la Commission dans sa communication du 18 avril 2023 sur l'Académie des compétences en matière de cybersécurité. Il importe de remédier à cette pénurie de talents en renforçant la coopération et la coordination entre les différentes parties prenantes, notamment le secteur privé, le monde universitaire, les États membres, la Commission et l'ENISA, afin de renforcer et de créer des synergies pour l'investissement dans l'éducation et la formation, le développement de partenariats public-privé, le soutien aux initiatives de recherche et d'innovation, le développement et la reconnaissance

mutuelle de normes communes et la certification des compétences en matière de cybersécurité, y compris au moyen du cadre européen pour les compétences en matière de cybersécurité. Ces mesures devraient également faciliter la mobilité des professionnels de la cybersécurité au sein de l'Union.

Or. en

Amendement 28
Johan Nissinen

Proposition de règlement
Considérant 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 bis) Étant donné que les schémas de certification accroîtront la complexité d'un paysage réglementaire déjà complexe, il est essentiel d'éviter d'éventuels chevauchements ou conflits avec les réglementations et normes existantes en matière de cybersécurité. La mise en œuvre du règlement demande en outre une réflexion approfondie et le respect de la proportionnalité, afin de réduire les effets négatifs sur la liberté du marché et l'innovation.

Or. en

Amendement 29
Josianne Cutajar

Proposition de règlement
Considérant 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 bis) Il convient de prévoir un financement et des ressources suffisants pour permettre à l'ENISA de mener à

bien les tâches supplémentaires qui lui sont confiées par le biais du présent acte législatif.

Or. en

Amendement 30
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 2 –sous-point a – partie introductive

Texte proposé par la Commission	*Amendement*
a) les points 9), 10) et 11) sont remplacés par le texte suivant:	a) les points ***7),*** 9), 10) et 11) sont remplacés par le texte suivant:

Or. en

Amendement 31
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point a
Règlement (UE) 2019/881
Article 2 – point 7

Texte proposé par la Commission	*Amendement*
	7) «gestion d'incident», la gestion d'incident au sens de l'article 6, point 8), de la directive (UE) 2022/2555;

Or. en

Amendement 32
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 2 –sous-point b – partie introductive

Texte proposé par la Commission	*Amendement*
b) ***le point suivant est inséré***:	b) ***les points suivants sont insérés***:

Or. en

Amendement 33
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) 2019/881
Article 2 – point 7 bis

Texte proposé par la Commission	*Amendement*
	7 bis) «risque», un risque au sens de l'article 6, point 9), de la directive (UE) 2022/2555;

Or. en

Amendement 34
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) 2019/881
Article 2 – point 14 bis

Texte proposé par la Commission	*Amendement*
14 bis) ***"service*** de sécurité ***géré"***, un service ***consistant à effectuer des activités liées à la gestion des risques en matière*** de ***cybersécurité, ou à fournir une assistance dans le cadre*** de ***ces activités, y compris la réaction aux incidents***, ***les tests d'intrusion***, ***les audits*** de ***sécurité et le conseil***;	14 bis) ***«service*** de sécurité ***géré»***, un service de ***sécurité géré au sens*** de ***l'article 6***, ***point 40)***, de ***la directive (UE) 2022/2555***;

Or. en

Amendement 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) 2019/881
Article 2 – point 14 bis

Texte proposé par la Commission	*Amendement*
14 bis) «service de sécurité géré», un service consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, y compris la ***réaction aux incidents, les tests d'intrusion, les audits de sécurité*** et le ***conseil***;	14 bis) «service de sécurité géré», un service ***géré*** consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, y compris la ***prévention ou la détection des incidents ainsi que la réponse apportée*** et le ***rétablissement à la suite de ceux-ci***;

Or. en

Amendement 36
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 2 – sous-point b
Règlement (UE) 2019/881
Article 2 – point 14 bis bis

Texte proposé par la Commission	*Amendement*
	14 bis bis) «fournisseur de services de sécurité gérés», un fournisseur de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555;

Or. en

Amendement 37
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Article 1 – alinéa 1 – point 6

Règlement (UE) 2019/881
Article 47 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le programme de travail glissant de l'Union inclut notamment une liste de produits TIC, services TIC et processus TIC ou de catégories de ceux-ci, ainsi que de services de sécurité gérés, qui sont susceptibles de bénéficier d'une inclusion dans le champ d'application d'un schéma européen de certification de cybersécurité.	2. Le programme de travail glissant de l'Union inclut notamment une liste de produits TIC, services TIC et processus TIC ou de catégories de ceux-ci, ainsi que de services de sécurité gérés, qui sont susceptibles de bénéficier d'une inclusion dans le champ d'application d'un schéma européen de certification de cybersécurité. ***Il convient d'inclure des mesures de soutien visant à évaluer les besoins en travailleurs qualifiés, les types de compétences et les parcours de formation existants, ainsi que des mesures visant à combler les lacunes constatées.***

Or. en

Justification

L'exercice visant à recenser les produits TIC, services TIC et processus TIC ou catégories de ceux-ci et les services de sécurité gérés doit s'accompagner d'une évaluation des compétences et de mesures visant à combler les lacunes.

Amendement 38
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Proposition de règlement
Article 1 – alinéa 1 – point 6
Règlement (UE) 2019/881
Article 47 – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) la disponibilité et le développement de schémas nationaux de certification de cybersécurité couvrant toute catégorie spécifique de produits TIC, services TIC, processus TIC ou services de sécurité gérés et, en particulier, en ce qui concerne le risque de fragmentation;	a) la disponibilité et le développement de schémas nationaux de certification de cybersécurité ***et de normes internationales et sectorielles*** couvrant toute catégorie spécifique de produits TIC, services TIC, processus TIC ou services de sécurité gérés et, en particulier, en ce qui concerne le risque de fragmentation;

Or. en

Justification

Le programme de travail glissant de l'Union devrait évaluer l'évolution non seulement des systèmes nationaux, mais aussi des normes sectorielles et internationales.

Amendement 39
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) 2019/881
Article 49 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7) À l'article 49, le paragraphe 7 est remplacé par le texte suivant:	***supprimé***
7. La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut adopter des actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui satisfont aux exigences des articles 51, 52 et 54. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.;	

Or. en

Amendement 40
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) 2019/881
Article 49 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7) La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut adopter des actes ***d'exécution*** prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui satisfont aux exigences des articles 51, 52 et 54. ***Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.;***	7) La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut adopter des actes ***délégués*** prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui satisfont aux exigences des articles 51, 52 et 54.
	(Cette modification s'applique à l'ensemble du texte. Son adoption impose des adaptations techniques dans tout le texte.)

Or. en

Justification

Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.

Amendement 41
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Proposition de règlement
Article 1 – alinéa 1 – point 7
Règlement (UE) 2019/881
Article 49 – paragraphe 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	7 bis. Avant d'adopter de tels actes délégués, la Commission, en coopération avec l'ENISA, réalise et publie une

analyse d'impact de la proposition de schéma européen de certification de cybersécurité. Lors de la préparation de cette analyse d'impact, la Commission procède à des consultations publiques et à des consultations avec le groupe de certification de la cybersécurité des parties prenantes et le groupe européen de certification de cybersécurité.

Or. en

Justification

Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.

Amendement 42
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 –alinéa 1 – point 7 bis (nouveau)
Règlement (UE) 2019/881
Article 49 – paragraphe 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	7 bis) Le paragraphe suivant est inséré:
	«7 bis. La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut adopter des actes délégués prévoyant un schéma européen de certification de cybersécurité pour les services de sécurité gérés qui satisfont aux exigences des articles 51, 52 et 54. Ces actes délégués sont adoptés conformément à la procédure visée à l'article 66 bis.»

Or. en

Amendement 43
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – alinéa 1 – point 9
Règlement (UE) 2019/881
Article 51 bis – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
b) faire en sorte que le fournisseur ait mis en place des procédures internes appropriées pour garantir que les services de sécurité gérés sont fournis à tout moment à un niveau de qualité très élevé;	b) faire en sorte que le fournisseur ait mis en place des procédures internes appropriées pour garantir que les services de sécurité gérés sont fournis à tout moment à un niveau de qualité ***et de fiabilité*** très élevé;

Or. en

Amendement 44
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – alinéa 1 – point 9
Règlement (UE) 2019/881
Article 51 bis – alinéa 1 – point g

Texte proposé par la Commission	*Amendement*
g) faire en sorte que les produits TIC, services TIC et processus TIC [et le matériel] déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ne contiennent pas de vulnérabilités connues et comprennent les dernières mises à jour de sécurité;***;***	g) faire en sorte que les produits TIC, services TIC et processus TIC [et le matériel] déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ***soient dotés de logiciels et d'équipements à jour,*** ne contiennent pas de vulnérabilités connues et comprennent les dernières mises à jour de sécurité;

Or. en

Amendement 45
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 9
Règlement (UE) 2019/881
Article 51 bis – alinéa 1 – point g

Texte proposé par la Commission	*Amendement*
g) faire en sorte que les produits TIC, services TIC et processus TIC ***[et le matériel]*** déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ne contiennent pas de vulnérabilités connues et comprennent les dernières mises à jour de sécurité;***;***	g) faire en sorte que les produits TIC, services TIC et processus TIC déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ne contiennent pas de vulnérabilités connues et comprennent les dernières mises à jour de sécurité;

Or. en

Amendement 46
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – alinéa 1 – point 13 –sous-point b – sous-point ii – sous-point a bis
Règlement (UE) 2019/881
Article 56 – alinéa 3 – alinéa 3 – point a

Texte proposé par la Commission	*Amendement*
a) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits TIC, services TIC, processus TIC ou services de sécurité gérés et sur les utilisateurs, ainsi que des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits TIC, services TIC, processus TIC ou services de sécurité gérés ciblés***;***;	a) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits TIC, services TIC, processus TIC ou services de sécurité gérés et sur les utilisateurs, ainsi que des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits TIC, services TIC, processus TIC ou services de sécurité gérés ciblés***, y compris les PME. La Commission veille à ce que les PME disposent d'un soutien financier suffisant***

pour la mise en œuvre des mesures par le biais de programmes existants de l'Union;

Or. en

Amendement 47
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Proposition de règlement
Article 1 – alinéa 1 – point 14
Règlement (UE) 2019/881
Article 57 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Sans préjudice du paragraphe 3 du présent article, les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte ***d'exécution adopté en application de l'article 49, paragraphe 7***. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister.	1. Sans préjudice du paragraphe 3 du présent article, les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte ***délégué***. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister. *(Cette modification s'applique à l'ensemble du texte. Son adoption impose des adaptations techniques dans tout le texte.)*

Or. en

Justification

Cette modification reflète la modification de l'article 49.

Amendement 48
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – alinéa 1 – point 16 bis (nouveau)
Règlement (UE) 2019/881
Article 66 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	16 bis) L'article suivant est inséré:
	Article 66 bis (nouveau)
	Exercice de la délégation
	1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
	2. Le pouvoir d'adopter des actes délégués visé à l'article 49, paragraphe 7 bis, est conféré à la Commission pour une période de cinq ans à compter du ... [date d'entrée en vigueur de l'acte législatif de base ou toute autre date fixée par les colégislateurs]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.
	3. La délégation de pouvoir visée à l'article 49, paragraphe 7 bis, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

6. Un acte délégué adopté en vertu de l'article 49, paragraphe 7 bis, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de [deux mois] à l'initiative du Parlement européen ou du Conseil.

Or. en

Amendement 49
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 17 – partie introductive
Règlement (UE) 2019/881
Article 67

Texte proposé par la Commission	*Amendement*
17) À l'article 67, les paragraphes 2 et ***3*** sont remplacés par le texte suivant:	17) À l'article 67, les paragraphes ***1,*** 2***,*** ***3*** et ***4*** sont remplacés par le texte suivant:

Or. en

Amendement 50
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 17
Règlement (UE) 2019/881
Article 67 – paragraphe 1

Texte proposé par la Commission	*Amendement*
	1 Au plus tard le 28 juin 2024, et tous les quatre ans par la suite, la Commission évalue l'incidence, l'efficacité et l'efficience de l'ENISA et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'ENISA et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'ENISA en réaction à ses activités. Lorsque la Commission estime que le maintien du fonctionnement de l'ENISA n'est plus justifié au regard des objectifs, du mandat et des tâches qui lui ont été assignés, elle peut proposer que les dispositions du présent règlement relatives à l'ENISA soient modifiées.

Or. en

Amendement 51
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 17
Règlement (UE) 2019/881
Article 67 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'évaluation porte également sur les effets, l'efficacité et l'efficience des dispositions du titre III du présent règlement au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union et à améliorer le	2. L'évaluation porte également sur les effets, l'efficacité et l'efficience des dispositions du titre III du présent règlement au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union et à améliorer le fonctionnement du marché intérieur**,**

fonctionnement du marché intérieur.	***notamment l'évaluation de la procédure et des délais conduisant à l'élaboration et à l'adoption des premiers schémas européens de certification de cybersécurité et la manière dont cette procédure pourrait être améliorée et accélérée pour les systèmes de certification ultérieurs***.

Or. en

Amendement 52
Evžen Tošenovský

Proposition de règlement
Article 1 – alinéa 1 – point 17
Règlement (UE) 2019/881
Article 67 – paragraphe 4

Texte proposé par la Commission	*Amendement*
	4. Au plus tard le 28 juin 2024, et tous les quatre ans par la suite, la Commission transmet le rapport d'évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d'administration. Les conclusions de ce rapport sont rendues publiques. Le rapport est accompagné au besoin d'une proposition législative.

Or. en