AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ

UNE EUROPE DIGNE DE CONFIANCE ET SÉCURISÉE SUR LE PLAN NUMÉRIQUE

Stratégie de l'ENISA

Juin 2020

UNE EUROPE DIGNE DE CONFIANCE ET SÉCURISÉE SUR LE PLAN NUMÉRIQUE

AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ

AVANT-PROPOS

Depuis plus de 15 ans, l'Agence de l'Union européenne pour la cybersécurité (ENISA) joue un rôle clé en aidant l'Union européenne à réaliser son ambition visant à renforcer la confiance et la sécurité numériques dans toute l'Europe, aux côtés des États membres et des institutions et agences de l'Union. En rapprochant les communautés, l'ENISA a contribué avec succès à améliorer le degré de préparation de l'Europe et ses capacités de réponse aux cyberincidents.

En parallèle, la numérisation de notre économie et de notre société s'est considérablement intensifiée, comme l'a démontré la crise de la COVID-19, durant laquelle le recours collectif massif à des solutions informatiques à distance s'est avéré indispensable au maintien de nombreuses activités. Cette crise a souligné à quel point les pirates informatiques exploitent notre dépendance à l'égard de ces technologies. Elle a également révélé à quel point les cybermenaces se sont diversifiées, passant d'attaques ciblées à de nouvelles formes de menaces massives visant des millions d'entreprises et de citoyens, avec notamment une recrudescence d'incidents provoqués par des rançongiciels sophistiqués. Le développement rapide des produits et services numériques, du service en nuage et de la vidéoconférence à la 5G et à l'intelligence artificielle, a entraîné dans son sillage de nouveaux défis à appréhender et à relever.

Du fait de son mandat permanent, de l'élargissement de ses fonctions et du renforcement de ses capacités, l'ENISA a plus que jamais un rôle de premier plan à jouer pour aider l'Union et ses États membres à relever ces défis, alors qu'une nouvelle ère s'ouvre pour la cybersécurité en Europe.

À cet effet, l'ENISA s'emploiera à anticiper les tendances pertinentes ainsi qu'à recenser les toutes dernières connaissances et compétences techniques pour les partager avec le plus grand nombre. Elle accompagnera la Commission européenne et les États membres afin d'aider les acteurs publics et privés ainsi que les citoyens à prévenir et à maîtriser les risques associés aux cyberincidents. Avec la mise en œuvre du cadre de certification de cybersécurité, l'ENISA contribuera à promouvoir un changement de paradigme en renforçant le niveau de sécurité des solutions numériques déployées en Europe. Elle améliorera ainsi le climat de confiance et aidera chacun à faire les bons choix. Par ailleurs, l'Agence soutiendra activement la communauté opérationnelle européenne de la cybersécurité par une coopération étroite et une préparation commune visant à réagir de concert lorsque le prochain cyberincident de grande ampleur frappera l'Europe.

À mesure que l'ENISA endossera son nouveau rôle, l'ouverture, l'agilité et la fiabilité seront les maîtres mots de ses opérations quotidiennes, auxquelles s'ajoutera une collaboration plus étroite avec les États membres et la Commission européenne dans l'harmonisation des approches. L'ENISA s'emploiera également à diminuer son empreinte environnementale dans le contexte de la crise climatique actuelle et à proposer un environnement de travail socialement responsable et inclusif.

Le présent document de stratégie, élaboré avec le concours de l'ensemble du personnel de l'ENISA, des membres de son conseil d'administration et de son groupe consultatif dans une démarche collaborative et inclusive, fixe clairement les objectifs qui orienteront les travaux de l'ENISA lors des prochaines années afin de relever les nombreux défis à venir.

Au nom du conseil d'administration

Jean-Baptiste Demaison
Président du conseil d'administration

Krzysztof Silicki
Vice-président du conseil d'administration

VISION

Une Europe digne de confiance et sécurisée sur le plan numérique

MISSION

L'Agence européenne pour la cybersécurité (ENISA) a pour mission de garantir un niveau élevé commun de cybersécurité dans l'Union, en coopération avec l'ensemble de la communauté. À cette fin, elle fait office de centre d'expertise en matière de cybersécurité, collectant et offrant des conseils et une assistance techniques indépendants de haut niveau en la matière aux États membres et aux organes de l'Union européenne. L'ENISA contribue à l'élaboration et à la mise en œuvre des politiques de l'Union relatives à la cybersécurité.

Notre objectif est de renforcer la confiance dans l'économie connectée, d'améliorer la résilience et la fiabilité des infrastructures et des services de l'Union, et de maintenir la sécurité numérique de notre société et de nos citoyens. Nous aspirons à être une organisation agile, axée sur les personnes et responsable sur les plans environnemental et social.

VALEURS

Esprit de communauté
L'ENISA collabore avec les communautés, en respectant leurs compétences et leur expertise, et cultive les synergies et la confiance pour accomplir sa mission au mieux.

Excellence
L'ENISA vise un niveau d'expertise de pointe dans ses activités, maintient les normes d'exploitation les plus élevées et évalue ses performances dans une volonté d'amélioration constante guidée par l'innovation et l'anticipation.

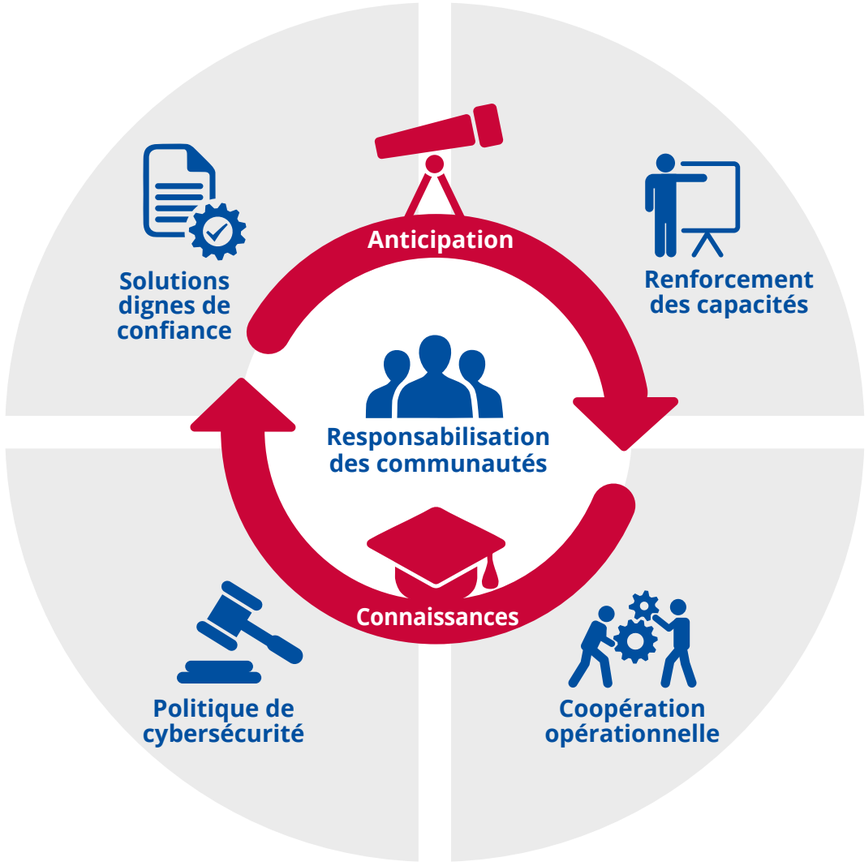
Intégrité/éthique
L'ENISA observe des principes éthiques ainsi que les règles et obligations applicables de l'Union dans ses activités et son environnement de travail, en garantissant l'équité et l'inclusion.

Respect
L'ENISA respecte les valeurs et les droits européens fondamentaux concernant l'ensemble de ses activités et son environnement de travail, ainsi que les attentes de ses partenaires.

Responsabilité
L'ENISA fait preuve de responsabilité en veillant à la prise en considération des dimensions sociale et environnementale dans ses pratiques et procédures.

Transparence
L'ENISA adopte des procédures, des structures et des processus ouverts, factuels et indépendants, réduisant ainsi le parti-pris, l'ambiguïté, la fraude et l'opacité.

OBJECTIFS STRATÉGIQUES



OS 1

Objectif stratégique

“

DES COMMUNAUTÉS AUTONOMES ET MOBILISÉES DANS L’ENSEMBLE DE L’ÉCOSYSTÈME DE CYBERSÉCURITÉ

Contexte

La cybersécurité est l’affaire de tous. L’Europe met tout en œuvre pour créer un cadre de coopération transversal et pleinement inclusif. L’ENISA joue un rôle clé dans la promotion d’une coopération active entre les acteurs de la cybersécurité au sein des États membres et des institutions et agences de l’Union. Elle s’emploie à garantir la complémentarité des efforts communs en valorisant les parties prenantes, en recherchant des synergies et en utilisant efficacement des compétences et des ressources limitées en matière de cybersécurité. Il convient de donner aux communautés les moyens de transposer à plus grande échelle le modèle de la cybersécurité.

Notre ambition

- Créer un pôle de connaissances de pointe à l’échelle de l’Union européenne sur les concepts et pratiques en matière de cybersécurité, à même de renforcer la coopération entre les principaux acteurs de la cybersécurité, de promouvoir les enseignements tirés, d’accroître l’expertise au sein de l’Union et de créer de nouvelles synergies.
- Bâtir un écosystème de la cybersécurité autonome englobant les autorités des États membres, les institutions, agences et organes de l’Union, les associations, les centres de recherche et les universités, l’industrie, les acteurs privés et les citoyens, qui jouent tous leur rôle pour assurer la cybersécurité de l’Europe.

OS 2

Objectif stratégique

LA CYBERSÉCURITÉ COMME PARTIE INTÉGRANTE DES POLITIQUES DE L'UNION EUROPÉENNE

Contexte

La cybersécurité est la pierre angulaire de la transformation numérique et les besoins en la matière concernent tous les secteurs; elle doit donc être intégrée dans un large éventail de champs d'action et d'initiatives stratégiques. La cybersécurité ne doit pas être réduite à une communauté spécialisée de techniciens experts en cybersécurité. Elle doit donc être intégrée à chaque domaine de la politique de l'Union. À cette fin, il sera essentiel d'éviter toute fragmentation et de mettre en œuvre une approche cohérente tout en tenant compte des spécificités propres à chaque secteur.

Notre ambition

- Conseiller et accompagner de manière proactive tous les acteurs concernés au niveau de l'Union, en intégrant le volet cybersécurité dans le cycle d'élaboration des politiques au moyen de lignes directrices techniques viables et ciblées.
- Mettre en place dans tous les secteurs des cadres de gestion des risques liés à la cybersécurité qui soient suivis tout au long du cycle d'élaboration des politiques en matière de cybersécurité.

OS 3

Objectif stratégique

UNE COOPÉRATION EFFICACE ENTRE LES ACTEURS OPÉRATIONNELS DE L'UNION EN CAS DE CYBERINCIDENT DE GRANDE AMPLEUR

Contexte

Les avantages de l'économie et de la société numériques européennes ne pourront être pleinement obtenus qu'à la faveur de la cybersécurité. Les cyberattaques ne connaissent pas de frontières. Toutes les strates de la société peuvent être touchées et l'Union doit se tenir prête à répondre à des crises de cybersécurité et à des cyberattaques massives (de grande ampleur et transfrontières). Les interdépendances transfrontières ont mis en évidence la nécessité d'une coopération efficace entre les États membres et les institutions de l'Union pour une réaction plus rapide et une coordination adéquate des efforts sur tous les plans (stratégique, opérationnel, technique et en matière de communication).

Notre ambition

- Fournir un appui transfrontière et multiniveaux constant à la coopération entre États membres ainsi qu'avec les institutions de l'Union. Compte tenu notamment des possibles incidents et crises de grande ampleur, appuyer l'intensification de la coopération technique, opérationnelle, politique et stratégique entre les principaux acteurs opérationnels pour favoriser une réaction rapide, le partage des informations, la connaissance de la situation et la communication de crise dans l'Union.
- Assurer un traitement technique complet et rapide, à la demande des États membres, pour faciliter la réponse aux besoins techniques et opérationnels en matière de gestion des incidents et des crises.

OS 4

Objectif stratégique

DES COMPÉTENCES ET DES CAPACITÉS DE POINTE EN CYBERSÉCURITÉ DANS L'ENSEMBLE DE L'UNION

Contexte

La fréquence et la sophistication des cyberattaques ne cessent de croître, tout comme l'utilisation des infrastructures et technologies de l'information et de la communication (TIC) par les citoyens, les organisations et le secteur privé. La demande de connaissances et de compétences en matière de cybersécurité excède l'offre. L'Union doit investir pour renforcer les compétences et former les talents en matière de cybersécurité à tous les niveaux, du non-expert au professionnel hautement qualifié. Ces investissements doivent viser non seulement à renforcer les compétences en matière de cybersécurité au sein des États membres, mais également à faire en sorte que les différentes communautés opérationnelles disposent des capacités adéquates pour faire face à l'ensemble des cybermenaces.

Notre ambition

- Mettre en adéquation les compétences, l'expérience professionnelle et les structures éducatives en matière de cybersécurité pour répondre aux besoins toujours plus importants au sein de l'Union s'agissant des connaissances et compétences dans ce domaine;
- Garantir un niveau de base élevé dans l'ensemble de l'Union en ce qui concerne la sensibilisation à la cybersécurité et les compétences dans ce domaine, tout en intégrant la question de la cybersécurité à de nouvelles disciplines;
- Mettre en place des capacités bien conçues et éprouvées permettant de faire face à un spectre de menaces en évolution dans l'ensemble de l'Union.

OS 5

Objectif stratégique

UN NIVEAU DE CONFIANCE ÉLEVÉ DANS DES SOLUTIONS NUMÉRIQUES SÉCURISÉES

Contexte

Les produits et services numériques comportent des avantages, mais également des risques, qu'il convient de cerner et d'atténuer. Dans le processus consistant à évaluer le degré de sécurité des solutions numériques et à garantir leur fiabilité, il est essentiel d'adopter une approche commune, avec pour objectif de trouver un équilibre entre les besoins inhérents à la société, au marché, à l'économie et en matière de cybersécurité. Une entité neutre agissant de manière transparente augmentera la confiance des utilisateurs dans les solutions numériques et l'environnement numérique au sens large.

Notre ambition

- Offrir dans toute l'Union un environnement numérique sécurisé sur le plan de la cybersécurité, dans lequel les citoyens peuvent avoir confiance dans les produits, services et processus TIC grâce au déploiement de schémas de certification dans des domaines technologiques clés.

OS 6

Objectif stratégique

L'ANTICIPATION DES DÉFIS NAISSANTS ET FUTURS EN MATIÈRE DE CYBERSÉCURITÉ

Contexte

De nombreuses nouvelles technologies, encore balbutiantes ou proches d'être adoptées par le grand public, gagneraient à s'appuyer sur des méthodes de prospective. Moyennant un processus structuré permettant le dialogue entre les parties prenantes, les décideurs et responsables politiques seraient en mesure de définir des stratégies d'atténuation précoce à même de renforcer la résilience de l'Union face aux cybermenaces, et de trouver des solutions pour faire face aux nouveaux défis.

Notre ambition

- Comprendre les tendances et les modèles naissants à l'aide de scénarios prospectifs qui contribuent à réduire les difficultés de nos parties prenantes en matière de cybersécurité;
- Anticiper les difficultés et les risques liés à l'adoption de solutions naissantes et futures ainsi qu'aux mesures d'adaptation nécessaires, tout en collaborant avec les parties prenantes à la formulation de stratégies d'atténuation appropriées.

OS 7

Objectif stratégique

UNE GESTION EFFICACE ET EFFICIENTE DES INFORMATIONS ET DES CONNAISSANCES RELATIVES À LA CYBERSÉCURITÉ EN EUROPE

Contexte

Les informations et les connaissances sont le carburant qui permet de faire progresser la cybersécurité. Pour que les professionnels de la cybersécurité puissent poursuivre efficacement nos objectifs, travailler dans un environnement en constante évolution – tant par ses acteurs que par ses technologies – et faire face aux défis de notre temps, nous devons mettre en place une démarche continue de collecte, d'organisation, de synthèse, d'analyse, de diffusion et de conservation des informations et des connaissances relatives à la cybersécurité. Toutes ces étapes sont essentielles en vue d'assurer le partage et l'approfondissement des informations et des connaissances dans l'écosystème de cybersécurité de l'Union.

Notre ambition

- Assurer une gestion partagée des informations et des connaissances relatives à l'écosystème de cybersécurité de l'Union sous une forme accessible, personnalisée, applicable et en temps utile, moyennant une méthodologie, des infrastructures et des outils appropriés, associés à des méthodes d'assurance qualité permettant une amélioration continue des services.

À PROPOS DE L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. Par le partage des connaissances, le renforcement des capacités et des initiatives de sensibilisation, l'Agence œuvre de concert avec ses parties prenantes principales pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et maintenir la sécurité numérique de la société européenne et de ses citoyens. De plus amples informations sur l'ENISA et ses travaux peuvent être consultées à l'adresse: www.enisa.europa.eu

TP-02-20-759-FR-N

ENISA
Agence de l'Union européenne pour la cybersécurité

Bureau d'Athènes
1 Vasilissis Sofias
151 24 Marousi, Attique, Grèce

Bureau d'Héraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Héraklion, Grèce

enisa.europa.eu