Cadre d'action de l'OCDE sur la sécurité numérique

LA CYBERSÉCURITÉ POUR LA PROSPÉRITÉ

OECD

Cet ouvrage est publié sous la responsabilité du Secrétaire général de l'OCDE. Les opinions exprimées et les arguments employés ici ne reflètent pas nécessairement les vues officielles des pays Membres de l'OCDE.

Veuillez citer cette publication comme suit:

OCDE (2022), *Cadre d'action de l'OCDE sur la sécurité numérique*, Éditions de l'OCDE, Paris, https://doi.org/10.1787/a0517600-fr

Note aux délégations :

Ce document est également disponible sur O.N.E sous la cote :

DSTI/CDEP/SDE(2021)12/FINAL

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

Crédit photo : Couverture © Zenzen/Shutterstock

© OCDE 2023

L'utilisation de ce document, sous forme numérique ou imprimée, est régie par les conditions générales d'utilisation consultables à l'adresse :

http://www.oecd.org/fr/conditionsdutilisation

Avant-propos

L'OCDE est à l'avant-garde des efforts déployés à l'échelle internationale pour guider les responsables de l'action publique dans le domaine de la sécurité numérique depuis 1990 et est devenue la principale instance internationale d'établissement de normes dans ce domaine. Les Recommandations de l'OCDE sur la sécurité numérique soutiennent les efforts des parties prenantes pour élaborer des politiques publiques au service de la prospérité économique et sociale, conformément à la mission de l'OCDE consistant à aider les pouvoirs publics à concevoir « des politiques meilleures pour une vie meilleure ».

Le Cadre d'action de l'OCDE sur la sécurité numérique vise à aider les responsables de l'action publique à comprendre la dimension économique et sociale de la cybersécurité, à les sensibiliser à l'approche des politiques de sécurité numérique définie par l'OCDE, et à les encourager à faire usage des recommandations de l'OCDE sur la sécurité numérique pour élaborer de meilleures politiques. Ce Cadre d'action offre un discours cohérent fondé sur les recommandations de l'OCDE relatives à la sécurité numérique, et met en évidence des liens avec d'autres domaines d'action auxquels se rapportent d'autres normes et outils de l'OCDE.

Le Cadre a également pour objet d'inciter les économies partenaires de l'OCDE intéressées à se joindre au dialogue international qui se déroule à l'OCDE dans ce domaine, et à aligner leurs politiques sur ces recommandations. Toutes les recommandations de l'OCDE couvertes par ce Cadre ont été élaborées par le biais d'un processus multipartite, avec la participation active du monde des affaires, de la société civile et de la communauté technique. Par conséquent, ce Cadre est également un outil destiné à faciliter un dialogue multipartite aux niveaux national et international.

Le Cadre a été rédigé par Laurent Bernat, avec la contribution de Ghislain de Salins, et sous la supervision d'Audrey Plonk, Chef de la division des politiques de l'économie numérique. Il a bénéficié des ajouts et commentaires des délégués du Groupe de Travail sur la Sécurité dans l'Economie Numérique et du Comité des Politiques de l'Economie Numérique.

© OCDE 2023

Table des matières

Avant-propos **3**

Introduction **5**

Contenu du Cadre 7
Replacer le Cadre dans un contexte plus général 10

1. Le niveau élémentaire : la cybersécurité au service de la prospérité **12**

1.1. Qu'est-ce que la sécurité numérique ? 12
1.2. Principes de gestion du risque de sécurité numérique 15

2. Le niveau stratégique : instaurer une culture de la sécurité numérique **22**

2.1. Objectifs et cadre institutionnel 22
2.2. Contenu de la stratégie 23

3. Le niveau du marché : renforcer la sécurité sans compromettre la prospérité **26**

3.1. Sécurité numérique des activités critiques 27
3.2. Sécurité numérique des produits et des services 30

4. Niveau technique : encourager les bonnes pratiques **33**

4.1. Traitement des vulnérabilités 33

Abréviations **37**

Références **38**

Notes **42**

GRAPHIQUES

Graphique 1. Vue d'ensemble du Cadre 8
Graphique 2. Sécurité numérique : la dimension économique et sociale de la cybersécurité 13
Graphique 3. Vue d'ensemble du cycle de gestion du risque 20
Graphique 4. Contenu de la Recommandation sur les activités critiques 28
Graphique 5. Types de mesures à l'intention des opérateurs 29
Graphique 6. Vue d'ensemble de la Recommandation sur les produits et les services 31
Graphique 7. Vue d'ensemble de la Recommandation sur les vulnérabilités 36

ENCADRÉS

Encadré 1. Préconiser une réponse responsable et dissuader les contre-attaques (« ripostes numériques ») 25
Encadré 2. Qu'est-ce qu'une activité critique ? 27
Encadré 3. Promouvoir des partenariats fondés sur la confiance 29
Encadré 4. Idées fausses courantes sur les vulnérabilités de sécurité numérique 34

© OCDE 2023

Introduction

La transformation numérique de plus en plus rapide de nos économies et de nos sociétés a des retombées positives remarquables pour les entreprises, les organisations du secteur public et les individus, allant des gains de productivité à l'amélioration du bien-être, en passant par un renforcement de la résilience face aux catastrophes majeures telles que la pandémie mondiale de COVID-19. Néanmoins, cette transformation a accentué notre dépendance numérique ainsi que la portée, l'ampleur et la complexité globale des systèmes d'information, des réseaux, des actifs de données et des flux de données des organisations. Celles-ci n'ont pas toujours suffisamment évalué le risque de sécurité numérique lié à cette évolution, ni pris des mesures de sécurité proportionnées pour le gérer. Les individus sont désorientés par la complexité du jargon technique, des dispositifs et des procédures relatifs à la cybersécurité, tels que les mises à jour, les procédures d'authentification, etc. Les produits et les services ne sont pas suffisamment sûrs et exposent leurs utilisateurs à des risques de sécurité, sans qu'ils aient accès aux informations et aux moyens nécessaires pour les atténuer. Des sources de menaces criminelles ou soutenues par des États tirent parti de cette situation, et renforcent leurs attaques dont ils retirent des gains financiers, politiques ou géopolitiques, entre autres. Selon des travaux de recherche récents, le coût mondial des cyberattaques serait compris entre 100 milliards et 6 000 milliards USD par an et tendrait à augmenter année après année (OCDE, 2021[1]). Tandis que les individus sont victimes d'usurpation d'identité, de fraude en ligne et de violations de données à caractère personnel, les entreprises sont confrontées à des cyberattaques qui portent préjudice à leurs actifs, leur réputation et leur compétitivité, et peuvent même déboucher sur des perturbations des chaînes d'approvisionnement mondiales, ainsi que l'ont montré les attaques WannaCry et NotPetya de 2017.

Dans ce contexte, la dimension économique et sociale de la cybersécurité devient une priorité pour les pouvoirs publics, à mesure qu'ils prennent conscience du fait que les forces du marché à elles seules ne suffisent pas à inciter les entreprises, les organisations du secteur public et les individus à mieux gérer le risque de sécurité numérique, selon leur rôle. Ainsi, des facteurs économiques tels que les externalités, les asymétries d'information et les incitations inadaptées empêchent souvent les développeurs de logiciels d'élaborer des produits « sûrs dès la conception » (OCDE, 2021[1]) et les organisations de renforcer leur gestion du risque de sécurité numérique et de s'attaquer de manière plus systématique à leurs vulnérabilités (OCDE, 2021[2]).

L'OCDE est une organisation internationale au sein de laquelle les responsables de l'action publique partagent leurs expériences et leurs bonnes pratiques, et établissent un dialogue fructueux avec le monde des affaires, la communauté technique et la société civile. L'OCDE produit également des analyses approfondies et des standards des politiques publiques dont la qualité est largement reconnue, qui sont fondées sur des éléments factuels, équilibrées et neutres. L'OCDE est à l'avant-garde des efforts déployés à l'échelle internationale pour guider les responsables de l'action publique dans le domaine de la sécurité numérique depuis 1990, bien avant qu'internet ne devienne un élément de la vie courante. Compte tenu de l'adoption au fil du temps de diverses recommandations[1] sur les politiques de sécurité numérique, l'OCDE est devenue la principale instance internationale d'établissement de normes dans ce domaine. Fondées sur des analyses approfondies, ces recommandations correspondent aux bonnes pratiques d'élaboration de politiques publiques relatives à la sécurité numérique au service de la prospérité

© OCDE 2023

économique et sociale, conformément à la mission de l'OCDE consistant à aider les pouvoirs publics à concevoir « des politiques meilleures pour une vie meilleure ».

Décrites de manière plus détaillée ci-après, ces recommandations sur la sécurité numérique sont des instruments juridiques internationaux adoptés par consensus par le Conseil de l'OCDE, et ouverts à l'adhésion d'économies partenaires de l'OCDE. Même si elles ne sont pas juridiquement contraignantes, les recommandations de l'OCDE représentent un engagement politique vis-à-vis des principes qu'elles contiennent, et l'on attend que les Adhérents fassent tout leur possible pour les mettre en œuvre.

Les recommandations sur la sécurité numérique visent à guider les responsables de l'action publique dans l'élaboration de stratégies et de politiques de sécurité numérique qui favorisent la confiance et la résilience, et étayent la transformation numérique, la compétitivité et la croissance, tout en protégeant les activités critiques, les droits humains et les valeurs fondamentales.

À la fin de 2022, cet ensemble de recommandations de l'OCDE sur la sécurité numérique comprendra sept recommandations élaborées depuis 1992 et actualisées au fil du temps. Ces recommandations vont probablement continuer à évoluer. D'autres pourraient également être élaborées dans l'avenir pour couvrir de nouveaux aspects de l'élaboration des politiques de sécurité numérique.

Les responsables publics de haut niveau et les acteurs non gouvernementaux ignorent trop souvent l'existence de ces recommandations de l'OCDE sur la sécurité numérique, de sorte que nombre d'entre eux ratent l'occasion de bénéficier des orientations qu'elles contiennent. La sécurité numérique, qui recouvre *la dimension économique et sociale de la cybersécurité*, est un domaine de l'action publique relativement récent, souvent relégué au second plan par les aspects de cette question liés à la sécurité nationale et internationale (« cyberdéfense », « cyberguerre », « cyberespionnage »), d'ordre technique (« sécurité de l'information ») et liés à l'application du droit pénal (« cybercriminalité ») (cf. section 1.1 Qu'est-ce que la sécurité numérique ?). En outre, compte tenu du nombre croissant d'instruments juridiques de l'OCDE dans ce domaine, il est possible que l'approche globale de l'OCDE en matière de sécurité numérique soit plus difficile à appréhender.

Le Cadre d'action de l'OCDE sur la sécurité numérique (dénommé ci-après le « Cadre ») a été rédigé par le Secrétariat pour offrir un discours cohérent fondé sur les recommandations de l'OCDE relatives à la sécurité numérique, et met en évidence des liens avec d'autres domaines d'action auxquels se rapportent d'autres normes et outils de l'OCDE.

Ce Cadre vise à aider les responsables de l'action publique à comprendre la dimension économique et sociale de la cybersécurité, à les sensibiliser à l'approche des politiques de sécurité numérique définie par l'OCDE, et à les encourager à faire usage des recommandations de l'OCDE sur la sécurité numérique pour élaborer de meilleures politiques. Il a également pour objet d'inciter les économies partenaires de l'OCDE intéressées à se joindre au dialogue international qui se déroule à l'OCDE dans ce domaine, et à aligner leurs politiques sur ces recommandations. Toutes les recommandations de l'OCDE couvertes par ce Cadre ont été élaborées par le biais d'un processus multipartite, avec la participation active du monde des affaires, de la société civile et de la communauté technique. Par conséquent, ce Cadre est également un outil destiné à faciliter un dialogue multipartite aux niveaux national et international.

En tant qu'outil de communication ciblé sur les responsables de l'action publique, le Cadre n'a pas pour objet de fournir une description détaillée et exhaustive de chacune des recommandations de l'OCDE sur la sécurité numérique. Il met en exergue quelques aspects essentiels de chaque recommandation et les présente de manière à les rendre aisément accessibles aux non-spécialistes. Il diffère également des normes techniques de sécurité numérique telles que celles élaborées par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI), par l'Institut européen de normalisation des télécommunications (ETSI) et par d'autres organismes internationaux de normalisation, ainsi que des cadres techniques nationaux ou régionaux de gestion des risques tels que le Cadre de cybersécurité de l'Institut national des normes et de la technologie (NIST, *National Institute of Standards*

© OCDE 2023

and Technologies) des États-Unis (NIST, 2018[3]). Néanmoins, l'OCDE a élaboré ses recommandations sur la sécurité numérique en cohérence avec ces normes techniques et en s'appuyant sur elles, de manière à faire la jonction entre les dimensions technique et politique. Les différences de public visé et de buts poursuivis peuvent expliquer en partie pourquoi la terminologie du Cadre peut occasionnellement ne pas être totalement en adéquation avec celle des normes techniques, qui sont elles-mêmes parfois incohérentes entre elles.

Contenu du Cadre

Le Cadre présente les recommandations suivantes :

- Recommandation sur la gestion du risque de sécurité numérique (dénommé ci-après la « Recommandation sur la sécurité numérique ») (OCDE, 2022[4]);
- Recommandation sur les stratégies nationales de sécurité numérique (dénommé ci-après la « Recommandation sur les stratégies ») (OCDE, 2022[5]) ;
- Recommandation sur la sécurité numérique des activités critiques (dénommée ci-après la « Recommandation sur les activités critiques ») (OCDE, 2019[6]) ;
- Recommandation sur la sécurité numérique des produits et des services (dénommé ci-après la « Recommandation sur les produits et les services ») (OCDE, 2022[7]) ;
- Recommandation sur la gestion des vulnérabilités de sécurité numérique (dénommé ci-après la « Recommandation sur les vulnérabilités ») (OCDE, 2022[8]);

Une prochaine version du Cadre couvrira également la Recommandation sur l'authentification électronique (OCDE, 2007[9]) et la Recommandation relative aux Lignes directrices régissant la politique de cryptographie (dénommée ci-après les « Lignes directrices sur la politique de cryptographie » (OCDE, 1997[10]).

Le Cadre est destiné à servir de point de départ pour la découverte de ces recommandations, et à faciliter leur diffusion. Il s'agit donc à dessein d'un document court, qui ne met en exergue qu'une fraction du contenu des recommandations auxquelles il se rapporte. Les lecteurs sont encouragés à explorer ces recommandations ainsi que les produits analytiques connexes de l'OCDE.[2]

Le Cadre est constitué de composantes axées sur des questions spécifiques, dont chacune est abordée dans une recommandation de l'OCDE. Ces composantes sont structurées en quatre niveaux, comme l'illustre le Graphique 1.

© OCDE 2023

Graphique 1. Vue d'ensemble du Cadre

Note : la politique de cryptographie et l'authentification électronique seront traitées dans la prochaine version du Cadre.
Source : OCDE.

- Le *niveau élémentaire* est le fondement de l'élaboration des politiques de sécurité numérique, sur lequel reposent tous les autres niveaux, à savoir la gestion du risque de sécurité numérique. Il recouvre les principes fondamentaux à garder à l'esprit pour aborder la cybersécurité sous l'angle économique et social, et pour instaurer *une culture de la sécurité numérique permettant de protéger les activités, les individus et la société sans compromettre les avantages et possibilités offerts par les technologies de l'information et des communications (TIC), ni le respect des droits humains.* Il est présenté dans la section la section 1.2 ci-après, et correspond à la *Recommandation sur la sécurité numérique*. Tous les autres niveaux de ce Cadre reposent sur ces principes de haut niveau.
- Le *niveau stratégique* se rapporte à la façon dont les responsables de l'action publique devraient utiliser le niveau élémentaire pour élaborer des stratégies nationales de sécurité numérique offrant une vision claire, afin de garantir que toutes les parties prenantes, des organismes publics aux organisations des secteurs public et privé, en passant par les individus, unissent leurs forces de manière cohérente et homogène. Il est présenté dans le Chapitre 2 et correspond à la *Recommandation sur les stratégies*. Outre le fait qu'elles permettent d'adopter une approche globale à l'échelle de l'administration dans son ensemble concernant la politique de sécurité numérique, les stratégies nationales de sécurité numérique facilitent la création d'interfaces et de synergies avec d'autres domaines de l'action publique, tels que la politique de l'économie numérique, la protection de la vie privée et des données, les politiques sectorielles (portant par exemple sur la finance, l'énergie, l'éducation ou les compétences) et la coopération internationale.
- Le *niveau relatif à la réglementation des marchés* se rapporte aux domaines dans lesquels l'intervention de la puissance publique est nécessaire, parce que les forces du marché sont insuffisantes pour aboutir au niveau optimal de sécurité numérique. L'intervention des pouvoirs publics est sans doute nécessaire sur de nombreux marchés pour renforcer la sécurité numérique dans l'ensemble de la société, mais jusqu'ici les Recommandations de l'OCDE se sont essentiellement focalisées sur les deux domaines suivants dans ses recommandations :

© OCDE 2023

- La sécurité numérique des activités critiques telles que les services financiers, les services de santé ou les services énergétiques, dont la perturbation ou la destruction affecterait le fonctionnement de l'économie et de la société, les vies humaines, ainsi que la sécurité nationale. La *Recommandation sur les activités critiques*, présentée dans le Chapitre 3, est axée sur la réglementation des opérateurs qui mènent à bien ces activités critiques, en vue de s'assurer que leur niveau de sécurité numérique est conforme au niveau de risque jugé acceptable par la société, et non uniquement par eux-mêmes.
- La sécurité numérique des produits contenant du code (informatique) et des services connexes – comme les services infonuagiques (*cloud computing*) – dont dépendent toutes les parties prenantes pour réaliser leurs activités économiques et sociales. Les travaux de l'OCDE montrent que le seul jeu des forces du marché est souvent insuffisant pour garantir que ces produits et services soient suffisamment sûrs, et qu'il est peu probable que les mécanismes d'incitation du marché puissent à eux seuls permettre de remédier aux insuffisances de ces produits et services en matière de sécurité numérique. La *Recommandation sur les produits et les services*, présentée ci-dessous dans la section 3.2, est axée sur les mesures destinées à remédier à ces défaillances du marché.

- Le *niveau technique* a trait à des aspects plus techniques exigeant des orientations à l'intention des pouvoirs publics. Il recouvre la nécessité d'encourager les parties prenantes à coordonner la divulgation des vulnérabilités de sécurité de leurs produits, à mieux gérer les vulnérabilités des systèmes d'information, et à protéger les chercheurs de vulnérabilités. La *Recommandation sur les vulnérabilités*, présentée dans le Chapitre 4, couvre ce domaine. La *politique de cryptographie* et l'*authentification électronique* devraient toutes deux être abordées dans une future version du Cadre, couvrant les *Lignes directrices de l'OCDE régissant la politique de cryptographie* de 1997 (OCDE, 1997[10]) et la *Recommandation de l'OCDE sur l'authentification électronique* de 2007 (OCDE, 2007[9]).

La sécurité numérique constitue un vaste domaine de l'action publique d'une ampleur croissante, et le Cadre ne porte que sur les domaines dans lesquels des recommandations ont été adoptées par l'OCDE. Par conséquent, même si le Cadre ne prétend pas à l'exhaustivité, il est susceptible d'être élargi et modifié, notamment dans la mesure où il pourrait être nécessaire de revoir les normes existantes de l'OCDE à la lumière de nouvelles évolutions. En outre, dans l'avenir, de nouvelles technologies ou de nouveaux problèmes techniques pourraient exiger des orientations spécifiques concernant les politiques de sécurité numérique, qui se traduiraient par l'ajout de composantes au niveau supérieur du Cadre. Des normes pourraient également être nécessaires pour traiter des problèmes posés sur certains marchés (comme le marché de l'emploi, ou des secteurs tels que l'énergie, la santé ou les assurances) ou affectant certaines catégories de parties prenantes, comme les petites et moyennes entreprises (PME). La Recommandation sur les stratégies nationales de sécurité numérique offre une vue d'ensemble plus complète de ces domaines d'action, dont bon nombre ne sont pas encore couverts par les recommandations de l'OCDE.

Il existe de nombreux liens entre les différentes composantes du Cadre, en sus de ceux déjà mentionnés. Ainsi, la sécurité numérique des produits et des services dépend en partie de la mesure dans laquelle les parties prenantes gèrent effectivement les vulnérabilités de sécurité numérique ; la protection des activités critiques suppose que les produits et les services soient suffisamment sûrs ; et de nombreuses mesures de sécurité techniques relatives aux produits ou aux activités critiques passent par des dispositifs efficaces de cryptographie et d'authentification électronique. Cartographier l'ensemble des liens pouvant exister nous amènerait à sortir du périmètre de ce document.

© OCDE 2023

Replacer le Cadre dans un contexte plus général

La sécurité numérique est un moyen d'atteindre des objectifs économiques et sociaux, et non une fin en soi. Il est donc important de concevoir et de mettre en œuvre des politiques de sécurité numérique qui soient cohérentes avec celles élaborées dans des domaines connexes de l'action publique. Lorsqu'elles sont conçues et/ou mises en œuvre isolément, les politiques de sécurité numérique risquent fort d'être incohérentes avec les politiques publiques d'autres domaines, et d'être perçues comme contraignantes, coûteuses et contre-productives. Lorsqu'elles visent à créer des synergies avec les objectifs poursuivis dans d'autres domaines de l'action publique, il est probable que les politiques de sécurité numérique soient plus efficaces. La *Recommandation sur les stratégies nationales* fournit de plus amples informations sur la façon d'élaborer des politiques de sécurité numérique à l'échelle de l'administration dans son ensemble.

Cette section met en lumière les principaux liens existants entre le Cadre et les domaines d'action dans lesquels l'OCDE a élaboré d'autres recommandations et outils. Elle vise à aider les responsables de l'action publique à utiliser les normes existantes de l'OCDE pour s'orienter dans le contexte général dans lequel s'inscrit l'élaboration des politiques de sécurité numérique, même s'il est clair que le périmètre de ce document ne permet pas de cartographier l'ensemble des liens pouvant exister entre le Cadre et tous les domaines de l'action publique. Le Cadre s'articule avec les recommandations et les outils de l'OCDE qui sont directement liés aux technologies numériques, comme :

- **Le Cadre d'action intégré du projet « Vers le numérique »** (dénommé ci-après le "Cadre du projet « Vers le numérique »") (OCDE, 2020[11]), qui réunit les dimensions de l'action publique nécessaires pour mettre la transformation numérique au service de la croissance et du bien-être, à savoir l'accès, l'utilisation, l'innovation, les emplois, la société, la confiance, l'ouverture des marchés et la stratégie. Plus précisément, la sécurité numérique est une composante essentielle de la dimension du Cadre du projet « Vers le numérique » que constitue la confiance, conjuguée par exemple à la protection des consommateurs et de la vie privée.
- **La Recommandation de l'OCDE concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel** (OCDE, 2013[12]) **(« Lignes directrices sur la vie privée »)**. La sécurité numérique fournit une base solide pour la mise en œuvre du Principe des garanties de sécurité énoncé dans les Lignes directrices de l'OCDE sur la vie privée, selon lequel il « conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés ». La sécurité numérique permet de s'assurer que les mesures de sécurité sont adaptées et proportionnées au risque, ce qui constitue une approche efficace de la formulation de mesures de sécurité « raisonnables ». Néanmoins, la sécurité numérique peut aussi nuire au respect de la vie privée si des garanties appropriées ne sont pas mises en place pour protéger les données à caractère personnel, par exemple lors de la surveillance des réseaux ou du partage d'informations relatives au risque avec des tierces parties[3].
- **La Recommandation de l'OCDE sur la protection du consommateur dans le contexte du commerce électronique** (OCDE, 2016[13]), qui préconise que les entreprises gèrent le risque de sécurité numérique et mettent en œuvre des mesures de sécurité propres à en réduire les effets préjudiciables en ce qui concerne la participation des consommateurs au commerce électronique. Elle inclut également des dispositions relatives aux mesures de sécurité applicables aux mécanismes de paiement.
- **La Recommandation de l'OCDE sur la connectivité à haut débit** (OCDE, 2021[14])(dénommée ci-après la « Recommandation sur le haut débit »), qui offre une feuille de route aux responsables de l'action publique et aux organismes de réglementation pour exploiter pleinement le potentiel de la connectivité au service de la transformation numérique et garantir un accès égal de tous les

© OCDE 2023

utilisateurs. La Recommandation sur le haut débit est structurée autour de cinq piliers, notamment la nécessité pour les pouvoirs publics de prendre « des mesures visant à garantir la résilience, la fiabilité, la sécurité et la haute capacité des réseaux ».

- **La Recommandation de l'OCDE sur l'intelligence artificielle (IA)** (OCDE, 2019[15]), qui promeut une intelligence artificielle innovante et digne de confiance, et respectueuse des droits humains et des valeurs démocratiques. En vertu de son principe intitulé « Robustesse, sûreté et sécurité », les acteurs de l'IA devraient « appliquer de manière continue une approche systématique de la gestion du risque, à chaque phase du cycle de vie des systèmes d'IA, afin de gérer les risques y afférents, notamment ceux liés au respect de la vie privée, à la sécurité numérique, à la sûreté et aux biais ».
- La **Recommandation de l'OCDE sur les enfants dans l'environnement numérique** (OCDE, 2021[16]), qui vise à aider les pays à trouver un juste équilibre entre la protection des enfants face aux risques en ligne, et la promotion des opportunités et des bienfaits du monde numérique. Elle contient des principes pour la promotion d'un environnement numérique sûr et bénéfique pour les enfants ainsi que des recommandations pour un cadre d'action publique, et elle souligne l'importance de la coopération internationale.

Certaines parties du Cadre axées sur la gestion des risques sont cohérentes avec :

- Les **Principes directeurs de l'OCDE à l'intention des entreprises multinationales** (OCDE, 2011[17]) (dénommés ci-après les « Principes directeurs EMN »)[4], qui correspondent aux attentes des pouvoirs publics à l'égard des entreprises en termes de conduite responsable. Les Principes directeurs EMN constituent la norme internationale la plus complète relative à la conduite responsable des entreprises. Ils couvrent tous les principaux domaines de responsabilité des entreprises, notamment les droits humains, les droits des travailleurs, la corruption, les intérêts des consommateurs, la science et la technologie, ainsi que la fiscalité. Les Principes directeurs EMN recommandent aux entreprises d'exercer une diligence raisonnable fondée sur les risques pour éviter et atténuer les effets négatifs liés à leurs activités, chaînes d'approvisionnement et autres relations d'affaires. Le Guide sur le devoir de diligence pour une conduite responsable des entreprises (OCDE, 2018[18])[5] aide concrètement les entreprises à mettre en œuvre les Principes directeurs EMN, en leur fournissant des explications en des termes simples concernant ses recommandations en matière de diligence raisonnable et les mesures à prendre pour leur mise en œuvre.
- **La Recommandation de l'OCDE sur les Principes de gouvernance d'entreprise** (OCDE, 2015[19]), également connu en tant que principes G20/OCDE sur la gouvernance d'entreprise, ont pour objet d'aider les responsables de l'action publique à évaluer et améliorer le cadre juridique, réglementaire et institutionnel organisant la gouvernance d'entreprise, afin de favoriser l'efficience économique, une croissance durable et la stabilité financière (OCDE, 2015[20]) (cf. section 1.2).

À mesure que les technologies numériques transforment la quasi-totalité des secteurs de l'économie, le risque de sécurité numérique devient une préoccupation des responsables de l'action publique dans un nombre grandissant de domaines et pour d'autres questions sectorielles, qui ne sont pas intrinsèquement liées aux technologies numériques et ne sont pas spécifiquement traitées dans les normes de l'OCDE, telles que les assurances ou les politiques à l'égard des PME.

Enfin, les recommandations de l'OCDE sur la sécurité numérique font partie d'un ensemble plus vaste de normes de haut niveau de l'OCDE axées sur la politique de l'économie numérique, qui réaffirment toutes le rôle clé joué par la sécurité numérique pour promouvoir la confiance dans un monde où le numérique prend une place grandissante. On peut citer à cet égard la *Déclaration sur l'économie numérique : innovation, croissance et prospérité sociale* (Déclaration de Cancún) de 2016 (OCDE, 2016[21]), la *Recommandation de l'OCDE sur les principes pour l'élaboration des politiques de l'Internet* de 2011 (OCDE, 2011[22]), ainsi que la *Déclaration de l'OCDE sur le futur de l'économie Internet* (Déclaration de Séoul) de 2008 (OCDE, 2008[23]).

© OCDE 2023

1. Le niveau élémentaire : la cybersécurité au service de la prospérité

Ce chapitre présente des concepts clés, qui définissent la sécurité numérique du point de vue de l'OCDE et aident à la distinguer de domaines connexes mais différents (section 1.1), et expose les principes de gestion du risque de sécurité numérique qui figurent dans la *Recommandation sur la sécurité numérique* (section 1.2).

1.1. Qu'est-ce que la sécurité numérique ?

La sécurité numérique est l'ensemble des mesures prises pour *gérer le risque de sécurité numérique* au service de la prospérité économique et sociale. Du point de vue de l'action publique, il peut être utile d'appréhender la sécurité numérique comme une dimension spécifique de la cybersécurité, avant de la définir plus précisément.

La sécurité numérique en tant que dimension économique et sociale de la cybersécurité

Sous l'angle international et du point de vue de l'action publique, la cybersécurité peut être considérée comme un vaste enjeu pluridimensionnel ayant pour objet de contribuer :

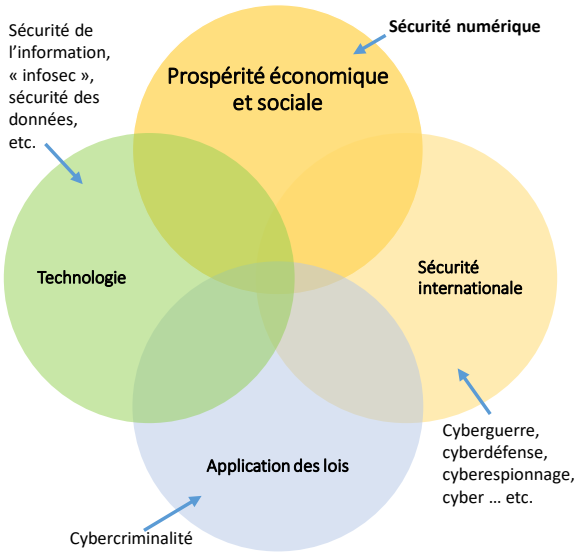
- Au bon déroulement des *opérations techniques*, en garantissant que les systèmes d'information fonctionnent comme prévu. C'est ainsi que la cybersécurité a vu le jour d'un point de vue historique, à savoir comme une question technique traitée par des experts qui la qualifient souvent de *sécurité informatique*, de *sécurité de l'information*, d'*« infosec »*, ou encore de *sécurité des données*.
- À la *prospérité*, en garantissant que la sécurité serve des objectifs économiques et sociaux (et non uniquement techniques). Cette dimension est axée sur le risque pesant sur les activités économiques et sociales fondées sur un environnement numérique, plutôt que sur la sécurité de l'environnement numérique lui-même. L'OCDE qualifie cette dimension de *sécurité numérique* ou de *gestion du risque de sécurité numérique*.
- À l'*application du droit pénal*, c'est-à-dire à la mise en œuvre de la législation relative à la *cybercriminalité* pour réduire les menaces. La cybercriminalité peut cependant recouvrir d'autres aspects que ceux présentés ci-dessous, tels que l'exploitation des enfants sur internet.
- À la *sécurité nationale et internationale*, par le biais de mesures de confiance et d'autres initiatives destinées à prévenir l'extension des conflits armés au cyberespace et à permettre une désescalade à cet égard. Cette dimension est souvent qualifiée de *cyberdéfense*, de *cyberguerre* ou de *cyberespionnage*.

© OCDE 2023

Ces objectifs ou dimensions de la cybersécurité se recoupent dans une certaine mesure et sont donc liés les uns aux autres, ainsi que l'illustre le Graphique 2.

Les pouvoirs publics ont adopté des cadres institutionnels divers pour élaborer et mettre en œuvre des mécanismes liés à chacune de ces dimensions, en s'appuyant sur différents organismes nationaux, avec des degrés divers de centralisation et de coordination avec d'autres organismes publics. Au niveau international, chaque dimension relève généralement de différentes organisations internationales, conformément à leurs missions respectives. Ainsi, l'OCDE aborde la question des politiques de sécurité numérique conformément à sa mission économique et sociale axée sur « des politiques meilleures pour une vie meilleure » ; des organisations de normalisation comme l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI), le Groupe de travail sur l'ingénierie internet (IETF) ou l'Institut européen de normalisation des télécommunications (ETSI), ou la Commission d'études 17 du secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications (UIT-T) élaborent des normes techniques ; le Conseil de l'Europe, l'Office des Nations unies contre la drogue et le crime (ONUDC) et Interpol (à un niveau plus opérationnel) se concentrent sur la cybercriminalité ; et le Groupe d'experts gouvernementaux ainsi que le Groupe de travail à composition non limitée des Nations unies examinent les questions de sécurité internationale.

Graphique 2. Sécurité numérique : la dimension économique et sociale de la cybersécurité



Source : OCDE.

Fondements de la sécurité numérique

Le risque de sécurité numérique est l'effet préjudiciable[6] que peuvent avoir les *incidents* de sécurité numérique sur les activités économiques et sociales. Comme tous les autres risques, le risque de sécurité numérique est caractérisé en termes de *probabilité* et d'*impact* (i.e. sévérité) potentiel des incidents[7]. La définition du risque qui figure dans les recommandations de l'OCDE sur la sécurité numérique s'inspire des normes ISO/IEC sur la gestion du risque et la sécurité de l'information[8]. Il est important de noter que l'objectif de la sécurité numérique est d'étayer la prospérité. Le renforcement de la sécurité numérique n'est pas une fin en soi.

© OCDE 2023

Les incidents de sécurité numérique sont des événements qui affectent la disponibilité, l'intégrité et/ou la confidentialité (triade DIC) des données, des logiciels, du matériel et des réseaux et, partant, entraînent des répercussions négatives sur les activités économiques et sociales fondées sur ces actifs :

- *Disponibilité* : les actifs ne sont pas accessibles et utilisables à la demande par les utilisateurs autorisés ;
- *Intégrité :* les actifs ont été altérés de manière non autorisée ;
- *Confidentialité :* des entités non autorisées ont accès aux actifs.

Ces incidents sont provoqués par des *menaces* exploitant des *vulnérabilités*. Les menaces peuvent être intentionnelles (comme une attaque) ou non intentionnelles (telles que des erreurs humaines, des incendies, des coupures de courant, etc.). Les menaces recouvrent les acteurs malveillants (les « sources de menaces ») prêts à exploiter les vulnérabilités pour nuire, ainsi que les outils et techniques (les « vecteurs de menaces ») auxquels ils recourent pour mener des attaques (tels que des logiciels malveillants). L'éventail des acteurs malveillants va d'individus aux compétences relativement limitées à des groupes criminels organisés et des acteurs soutenus par des États, dotés de ressources considérables, souvent qualifiés de menaces persistantes avancées. Les attaques appuyées par des États sont généralement motivées par des objectifs géopolitiques, et les actes de cybercriminalité par un objectif de gains financiers. Certains acteurs poursuivent également des buts idéologiques (comme les « hacktivistes »). Dans de nombreux cas, il peut être extrêmement difficile d'attribuer avec précision les attaques à des individus, des groupes ou ceux qui les soutiennent sur la seule base de leur mode opératoire ou d'éléments d'expertise scientifique, en partie parce que des acteurs malveillants dotés de ressources considérables peuvent imiter le mode opératoire d'autres sources de menaces. Les menaces exploitent les *vulnérabilités* des individus (telles que le manque de formation et de sensibilisation), des processus (comme l'absence de procédure de sauvegarde ou d'administration systématique des vulnérabilités) et des technologies (telles que les failles présentes dans les codes logiciels).

Pour l'OCDE, le risque de sécurité numérique désigne le risque économique et social, plutôt que le risque technique, résultant des incidents. Les deux sont liés, mais il faut les distinguer. Le risque économique et social résulte du risque technique. Le risque technique se limite aux éventuelles atteintes à la triade DIC et à des éléments liés aux technologies de l'information et des communications (TIC), tels que les défaillances des systèmes, les périodes d'indisponibilité, les accès non autorisés, les pertes d'actifs numériques, etc. En revanche, les conséquences économiques et sociales de ces atteintes peuvent prendre la forme de pertes financières, de coûts d'opportunité, d'atteintes à la réputation, de vols de propriété intellectuelle, de violations de la vie privée et d'atteintes à la sécurité des personnes. Ainsi, lorsqu'un rançongiciel touche un hôpital et se diffuse sur le réseau, certains systèmes d'information infectés peuvent devenir indisponibles et il peut être nécessaire d'en arrêter d'autres pour atténuer la gravité de l'incident (risque technique). En conséquence, des patients opérés au moment où l'incident se produit peuvent être mis en danger parce qu'un équipement médical cesse de fonctionner, et des interventions chirurgicales programmées risquent de devoir être reportées (risque économique et social). D'après une enquête de 2021 menée par l'institut de sondage Ponemon, 22 % des professionnels de l'informatique et de la sécurité informatique travaillant pour des prestataires de soins de santé estimaient qu'une attaque par rançongiciel entraînait une augmentation du taux de mortalité[9].

La gestion du risque de sécurité numérique désigne les mesures prises par les individus et les organisations pour maîtriser ce risque tout en maximisant leurs possibilités économiques et sociales. La gestion du risque consiste en son évaluation puis son traitement, qui peut consister à réduire, éviter, transférer ou prendre le risque considéré (on trouvera de plus amples informations en 1.2 ci-après). Nous gérons le risque en permanence, même si nous n'en avons pas conscience. Ainsi, quand nous voulons traverser une rue, nous vérifions si des voitures ou des vélos arrivent, afin d'*évaluer* le risque avant de décider ce que nous allons faire. S'il s'agit d'une autoroute, nous nous abstenons de la traverser

© OCDE 2023

afin d'*éviter* le risque, qui est trop élevé. Pour *réduire* le risque, nous empruntons les passages piétonniers, et nous souscrivons une police d'assurance pour *transférer* le risque, « au cas où ». Si nous traversons simplement la rue sans évaluer le risque, par exemple alors que nous marchons tout en effectuant plusieurs tâches sur un smartphone, nous *acceptons* tout simplement le risque, et nous devrons en assumer les conséquences. *L'évaluation du risque est absolument essentielle pour la sécurité*, y compris la sécurité numérique. Il est parfaitement recevable d'accepter un risque après une évaluation attentive et systématique, mais son acceptation aveugle sans évaluation du risque considéré est une attitude irresponsable.

La gestion du risque de sécurité numérique permet d'ancrer les décisions de sécurité numérique dans la réalité économique et sociale de l'activité concernée. Elle permet de choisir des mesures de sécurité appropriées et proportionnées à la fois au risque et à l'activité. Ce faisant, *elle permet de s'assurer que les mesures de sécurité adoptées soutiendront les activités économiques et sociales en jeu, et ne les compromettront pas*, par exemple, en fermant de manière inappropriée l'environnement ou en réduisant la fonctionnalité des TIC d'une manière qui limite la possibilité de tirer parti de ces technologies pour innover et accroître la productivité. La gestion du risque de sécurité numérique permet d'éviter une prise de décision isolée, fondée exclusivement sur des critères techniques ou de sécurité (la sécurité étant alors une fin en soi).

Le risque de sécurité numérique est une forme particulière de risque numérique, qui n'est lui-même qu'un des nombreux risques auxquels est confrontée une personne ou une organisation lorsqu'elle utilise des technologies numériques. Tous les risques sont liés entre eux et par conséquent la gestion du risque ne devrait pas être approchée en silo. Les autres risques numériques recouvrent tous les problèmes pouvant survenir dans l'environnement numérique, de la mésinformation à la désinformation, en passant par la fraude (comme la compromission de courriels professionnels), l'exploitation des enfants sur internet, etc. Il peut certes exister des points de jonction entre le risque de sécurité numérique et d'autres risques numériques, mais il importe d'éviter toute confusion et de ne pas amalgamer ces deux catégories distinctes, en particulier dans le contexte de la prise en compte du risque de sécurité numérique au niveau international.

1.2. Principes de gestion du risque de sécurité numérique

Cette section présente les neuf principes de haut niveau étroitement liés qui constituent le fondement d'une approche économique et sociale efficace de la cybersécurité, et figurent dans la *Recommandation sur la sécurité numérique* de l'OCDE. Toutes les autres recommandations de l'OCDE sur la sécurité numérique reposent sur ces principes.

Ces principes sont au cœur d'une *culture de la sécurité numérique* pour les responsables de l'action publique ainsi que pour les dirigeants et les décideurs des organisations publiques et privées, qui poursuivent les mêmes buts : protéger des cybermenaces les activités qui reposent sur l'environnement numérique *i)* sans entraver ces activités, brider l'innovation, faire obstacle à la transformation numérique ni compromettre les droits humains, *ii)* tout en tenant compte du caractère dynamique des technologies, des activités économiques qui en dépendent, et des menaces qui les entourent. Ces principes pourraient également être utiles aux individus, même si leur capacité à agir est généralement limitée.

Les principes généraux brièvement présentés ci-après sont destinés à toutes les parties prenantes, tandis que les principes opérationnels s'adressent aux dirigeants et aux décideurs des organisations. Le texte en italique dans les encadrés est un bref extrait de la *Recommandation sur la sécurité numérique*, qui contient des informations plus détaillées[10].

© OCDE 2023

Principes généraux

1. Culture de la sécurité numérique : sensibilisation, compétences et autonomisation	*Toutes les parties prenantes devraient instaurer une culture de la sécurité numérique fondée sur la compréhension du risque de sécurité numérique et de sa gestion.*
2. Responsabilité et obligations	*Toutes les parties prenantes devraient assumer la responsabilité de la gestion du risque de sécurité numérique, selon leur rôle, le contexte et leur capacité à agir.*
3. Droits humains et valeurs fondamentales	*Toutes les parties prenantes devraient gérer le risque de sécurité numérique de manière transparente, dans le respect des droits humains et des valeurs fondamentales.*
4. Coopération	*Toutes les parties prenantes devraient coopérer, y compris par-delà les frontières.*

Une culture de la sécurité numérique est essentielle pour gérer le risque de sécurité numérique (Principe 1). C'est dans en gardant cette idée fondamentale à l'esprit que les parties prenantes devraient aborder la question de la sécurité numérique, que ce soit pour élaborer et mettre en œuvre les politiques publiques ou pour protéger leur organisation – entreprise, organisme public, organisation non gouvernementale (ONG) – leurs actifs personnels et leur sécurité, sans compromettre les avantages et possibilités offerts par les TIC, ni le respect des droits humains.

Premièrement, **il est essentiel d'avoir conscience de l'existence du risque de sécurité numérique, et d'acquérir les compétences appropriées** – par l'éducation, la formation, l'expérience ou la pratique – pour être en mesure de prendre des décisions responsables (autonomisation). Si les conséquences possibles d'un accident de voiture sont intuitives, la complexité de l'environnement numérique brouille le lien entre l'incident et ses conséquences. Ainsi, bien que de nombreuses personnes soient conscientes du fait qu'un virus peut infecter leur équipement, elles n'en mesurent pas les conséquences potentielles telles que l'usurpation d'identité, la fraude financière ou le vol de secret commercial. Les conséquences pour autrui sont encore moins visibles, par exemple lorsqu'un équipement infecté vient à faire partie d'un botnet (réseau d'ordinateurs compromis) utilisé pour lancer des attaques par déni de service sur des tierces parties. La sensibilisation au risque de sécurité numérique devrait donc mettre l'accent sur les effets économiques et sociaux potentiels (autrement dit, les risques) des incidents, et non uniquement sur les facteurs de risque comme les menaces et les vulnérabilités.

Une règle fondamentale de notre vie sociale est que chacun doit assumer les conséquences de ses actes, y compris sur autrui. **Nous assumons donc tous la responsabilité partagée de nos décisions en matière de sécurité numérique**, ou de leur absence (Principe 2). Néanmoins, la nature et le degré de cette responsabilité varient selon le *rôle* des différentes parties prenantes. Ainsi, la responsabilité de l'utilisateur d'un appareil numérique est différente de celle du vendeur de cet appareil, de son fabriquant, des tierces parties ayant développé les composants logiciels incorporés dedans, des fournisseurs de services infonuagiques hébergeant les données traitées par l'appareil, etc. Le *contexte* est également important. Ainsi, la responsabilité des concepteurs, des vendeurs ou des utilisateurs de logiciels ou d'appareils est différente si le produit considéré est utilisé à des fins de divertissement (comme les jeux en ligne), dans un environnement médical (par exemple pour vérifier le niveau d'insuline) ou dans d'autres contextes critiques (valve connectée sur un pipeline, par exemple). Enfin, il faut prendre en compte la *capacité à agir* des parties prenantes. Ainsi, le consommateur moyen ne peut utiliser des produits de manière responsable si ceux-ci n'intègrent pas des dispositifs de sécurité élémentaires faciles à utiliser (comme l'authentification multifactorielle) et des paramètres de sécurité dans leur configuration (tels que des mises à jour automatiques). Les utilisateurs ne sont pas aptes à traiter les vulnérabilités d'un produit durant sa phase de conception. La capacité à agir de groupes spécifiques comme les consommateurs

© OCDE 2023

vulnérables (qui peuvent être des enfants, des personnes âgées, handicapées ou défavorisées) ou les organisations ayant des ressources limitées (comme les PME, les collectivités locales, les ONG, les hôpitaux, etc.) doit être prise en compte dans la perspective de la responsabilité et des obligations. La responsabilité vis-à-vis d'autrui est au cœur des recommandations de l'OCDE relatives à la diligence raisonnable fondée sur les risques qui figurent dans les Principes directeurs EMN[11] (OCDE, 2011[24]) et dans le Guide de l'OCDE sur le devoir de diligence pour une conduite responsable des entreprises (OCDE, 2018[18]). Bien que ces principes ne portent pas spécifiquement sur la sécurité numérique, ils peuvent constituer une ressource utile pour connaître les meilleures pratiques de haut niveau quant à la façon dont les parties prenantes peuvent exercer une diligence raisonnable fondée sur les risques, notamment en fournissant des orientations précises sur l'association des parties prenantes et la communication d'informations concernant leurs efforts d'évaluation et d'atténuation des risques.

Les droits en vigueur « hors ligne » doivent également s'appliquer en ligne. Par conséquent, **les droits humains et les valeurs fondamentales doivent être protégés dans l'environnement numérique** (Principe 3). Selon leurs modalités d'utilisation, les mesures de sécurité peuvent *favoriser ou compromettre* le respect des droits humains et des valeurs fondamentales. Ainsi, certaines mesures de sécurité peuvent contribuer à renforcer la protection de la vie privée, assurer l'anonymat des lanceurs d'alerte et protéger les défenseurs des droits humains contre la surveillance d'un régime autoritaire. Elles peuvent en revanche permettre une surveillance illégitime de citoyens ou d'employés, ou empêcher l'accès aux contenus produits par des militants. Une approche responsable de la sécurité numérique exige que les décisions de gestion du risque de sécurité numérique soient prises à la lumière de leurs conséquences sur ces droits et valeurs.

L'interconnexion mondiale qui caractérise l'environnement numérique permet certes d'en tirer des avantages économiques et sociaux considérables, mais elle se traduit aussi par une complexité accrue, facilite la propagation des menaces et des vulnérabilités, et accentue le risque collectif. **La coopération est essentielle aux niveaux national et international** pour remédier à ces inconvénients (Principe 4). Isolément, les parties prenantes ne peuvent réussir à traiter la question de la sécurité numérique. Ainsi, les dirigeants et les décideurs des organisations doivent coopérer avec des experts techniques pour évaluer le risque de sécurité numérique, et les experts techniques doivent coopérer avec ces responsables pour garantir que les mesures de sécurité techniques ne compromettent pas les objectifs et les activités de leur organisation. Une coopération s'impose également à l'intérieur et entre organisations, par exemple pour partager des informations sur la diffusion des menaces et des vulnérabilités à la fois dans une organisation et parmi ses partenaires, le long des chaînes d'approvisionnement ou au sein des administrations publiques, entre les organisations du même secteur économique, y compris entre concurrents (par exemple *via* les centres d'échange et d'analyse d'informations - ISACs), entre les secteurs publics et privés, les organisations et leurs consommateurs ou usagers et, de manière plus générale, la société civile. De même, l'élaboration et la mise en œuvre des politiques publiques sont plus efficaces lorsqu'elles sont étayées par des experts issus du monde des affaires, de la communauté technique et de la société civile.

Principes opérationnels

Les principes opérationnels portent sur la mise en œuvre de la gestion du risque de sécurité numérique dans les organisations. Ces principes s'appuient sur les fondements de la sécurité numérique présentés ci-dessus à la section 1.1.

5. Stratégie et gouvernance	*Les dirigeants et les décideurs devraient veiller à ce que le risque de sécurité numérique soit pris en compte dans leur stratégie globale de gestion du risque et géré en tant que risque stratégique appelant des mesures opérationnelles.*

© OCDE 2023

6. Évaluation et traitement du risque	*Les dirigeants et les décideurs devraient s'assurer que le traitement du risque de sécurité numérique se fonde sur une évaluation continuelle du risque.*
7. Mesures de sécurité	*Les dirigeants et les décideurs devraient s'assurer que les mesures de sécurité sont adaptées et proportionnées au risque.*
8. Innovation	*Les dirigeants et les décideurs devraient s'assurer que l'innovation est prise en considération.*
9. Résilience, préparation et continuité	*Les dirigeants et les décideurs devraient veiller à adopter, mettre en œuvre et tester un plan de préparation et de continuité fondé sur l'évaluation du risque de sécurité numérique, afin d'assurer la résilience.*

La première étape à suivre pour gérer le risque de sécurité numérique dans les organisations consiste à adopter une **approche stratégique** et à **mettre en place une gouvernance appropriée** (Principe 5). Il est primordial d'intégrer la gestion du risque de sécurité numérique dans le cadre général de gestion du risque de l'organisation (que l'on appelle souvent « gestion du risque d'entreprise ») afin que les décisions concernant la sécurité numérique soient inspirées par des objectifs économiques plutôt que par de simples considérations techniques, et qu'elles obéissent aux bonnes pratiques établies en matière de gestion du risque (approche systématique, cycle d'amélioration continue, etc.). Le conseil d'administration de l'entreprise a un rôle clairement défini dans la gestion du risque de sécurité numérique, conformément au chapitre sur les conseil d'administration des *Principes de gouvernance d'entreprise du G20 et de l'OCDE,* qui énonce que l'une des fonctions essentielles du conseil d'administration est de fixer les politiques de gestion des risques et de s'assurer de « l'intégrité des systèmes de comptabilité et de communication financière de la société, notamment [...], et que l'entreprise est dotée de dispositifs de contrôle adéquats, en particulier de dispositifs de gestion des risques [...] » (Principe VI.D.7) (OCDE, 2015[20]).

La structure de gouvernance devrait définir clairement les rôles, les responsabilités et les processus et prévoir des ressources et des compétences appropriées. *Les dirigeants et les décideurs responsables de la réalisation des objectifs économiques et sociaux devraient être responsables de la prise en charge du risque de sécurité numérique inhérent à ces activités (« appropriation du risque »).* Les risques et les bénéfices sont intrinsèquement mêlés, les risques affectant, par définition, les bénéfices de toute activité. Étant donné que la gestion du risque constitue un moyen d'accroître les chances de réussite d'une activité, les dirigeants et décideurs de l'organisation qui sont responsables des bénéfices de cette activité devraient l'être également du traitement du risque de sécurité numérique lui étant inhérent. Elles devraient travailler en coopération avec les spécialistes de la sécurité, qui sont responsables du risque de sécurité technique et peuvent les aider à comprendre comment celui-ci peut influer sur le risque économique et comment ces deux risques peuvent être réduits, notamment par des mesures techniques. Dans les grandes organisations, les experts de la sécurité peuvent se regrouper dans un comité technique, qui peut également inclure d'autres experts (juristes, communicants, etc.). Pour autant, dirigeants et décideurs ne doivent pas se contenter de déléguer à des spécialistes techniques la responsabilité de gérer le risque de sécurité numérique. La gestion du risque de sécurité numérique et les prise de décision afférentes requièrent une prise en compte holistique des activités de l'organisation et des conséquences que le risque peut avoir pour toutes les parties prenantes. S'il est essentiel d'instaurer une communication efficace et régulière entre les dirigeants (le PDG et le conseil d'administration dans le secteur privé, par exemple) et les équipes spécialisées dans la sécurité technique des systèmes informatiques, la gestion du risque devrait relever d'un processus décisionnel métier (et pas seulement technique) pour les raisons suivantes :

- *Les conséquences économiques et sociales des incidents de sécurité numérique peuvent être bien plus graves que leur coût technique (autrement dit, informatique)* pour l'organisation concernée et ses partenaires et pour les tiers. Les patients d'un hôpital, par exemple, risquent de décéder parce que des fichiers stockés sur des disques durs auront été chiffrés à l'aide de rançongiciels. Les investissements pluriannuels dans la recherche-développement risquent d'être

© OCDE 2023

gâchés si un concurrent parvient à s'emparer de la propriété intellectuelle d'une entreprise, avant que celle-ci ait pu déposer ses demandes de brevet. Le coût technique est généralement très en deçà du montant de ces investissements et de ces pertes de chances.

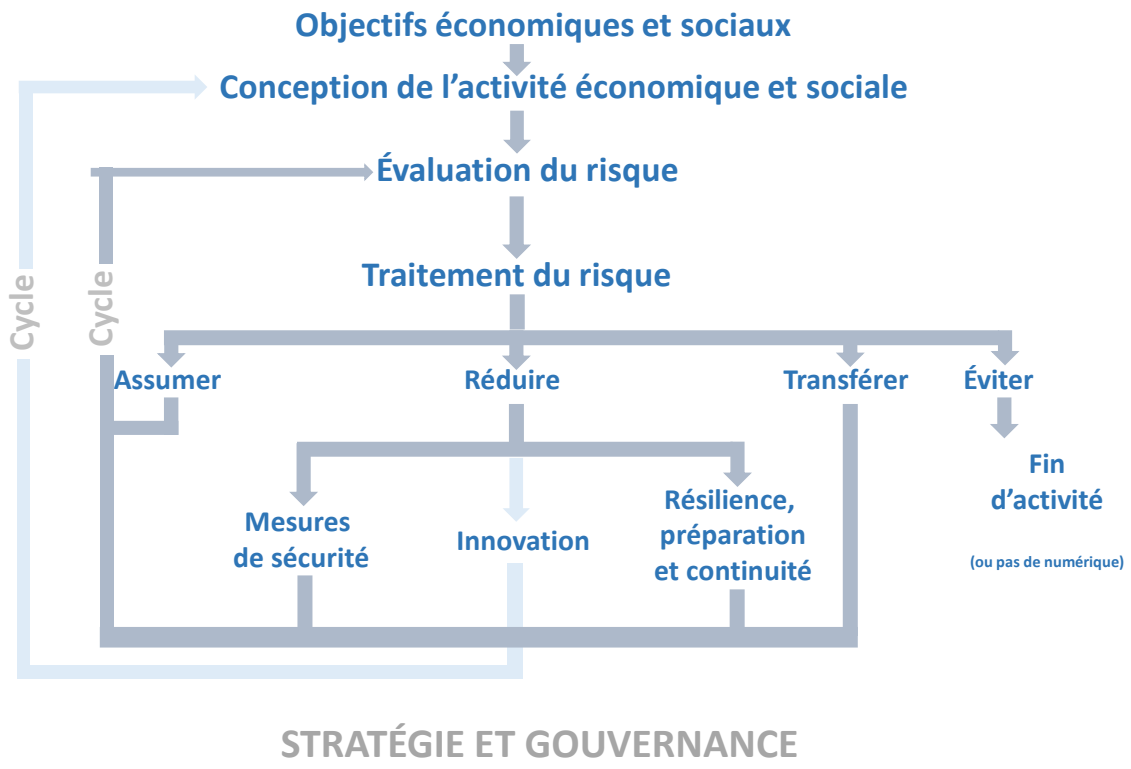
- *Les mesures de sécurité peuvent compromettre l'activité qu'elles visent à protéger.* Elles peuvent créer des obstacles à cette activité et des contraintes, notamment en accroître le coût financier et la complexité du système, allonger les délais de mise sur le marché, limiter les performances, la facilité d'utilisation, la capacité d'évolution, l'innovation, ou encore le confort d'utilisation. Elles peuvent également susciter des menaces pour la vie privée et avoir d'autres conséquences sociales préjudiciables. Ces contraintes et effets néfastes peuvent être traités et atténués, moyennant toutefois un certain coût.

Chaque activité est exposée à des incertitudes, qui peuvent minorer ses chances de succès. Pour accroître la probabilité de réussite, un **cycle d'évaluation et de traitement du risque** (Principe 6) permet d'aborder la question des incertitudes. Ainsi qu'il ressort du Graphique 3, la première étape du processus consiste à définir les objectifs et concevoir les activités qui reposent sur l'environnement numérique. Le risque est ensuite *évalué* pour calculer sa probabilité et les effets possibles des incertitudes sur les objectifs de l'activité. À la lumière de ce processus d'évaluation, une décision est prise sur ce qu'il convient de faire du risque (*traitement* du risque), autrement dit s'il convient de le modifier et dans l'affirmative, comment, de manière à accroître les chances de succès des activités menées à l'appui des objectifs visés et de leur maintien. Ce processus de traitement du risque permet de déterminer quelle part du risque devrait être :

- **Assumée** (ou prise, acceptée), celui-ci étant inférieur au niveau que l'entité juge acceptable pour mener son activité, ce que l'on désigne par « appétence pour le risque » ou « tolérance au risque ». Assumer ce risque signifie que l'on en accepte les conséquences économiques et sociales préjudiciables en cas d'incident.
- **Évitée**, sachant qu'il n'est pas possible d'éliminer intégralement le risque de sécurité numérique sans renoncer en même temps aux avantages de l'utilisation des TIC. En d'autres termes, le meilleur moyen d'éviter le risque de sécurité numérique est de s'abstenir d'utiliser les technologies numériques.
- **Réduite** au niveau acceptable en fonction de l'appétence pour le risque de l'entité, en mettant en place des mesures de sécurité qui préviennent la survenue d'incidents. Toutefois, des événements préjudiciables peuvent toujours se produire, en dépit des mesures de sécurité mises en place. Il est impossible de créer un environnement numérique entièrement sûr et sécurisé. Il subsistera toujours un « risque résiduel », qui ne peut être éliminé et doit être accepté. C'est la raison pour laquelle il est primordial de créer de la résilience et d'assurer la continuité des opérations, afin de se tenir toujours prêt à la survenue d'incidents éventuels et à la réduction de leurs conséquences.
- **Transférée** à un tiers, au moyen d'une assurance par exemple, s'il existe une offre de marché en la matière.

© OCDE 2023

Graphique 3. Vue d'ensemble du cycle de gestion du risque



Source : OCDE.

Un processus systématique et cyclique continu d'évaluation du risque est essentiel pour que les dirigeants et les décideurs puissent prendre des décisions éclairées sur le traitement à y apporter, qui soient adaptées à la nature constamment changeante du risque, les menaces, les vulnérabilités, les incidents, les technologies, leur utilisation et leurs bénéfices - pour ne citer que quelques-unes des variables de l'équation des risques d'une activité - évoluant extrêmement vite. L'évaluation du risque doit tenir compte des risques liés aux fournisseurs et aux partenaires avec lesquels l'organisation est interconnectée. Les décisions de traitement du risque qu'il est possible de prendre (assumer, réduire, transférer, éviter le risque) impliquent que les dirigeants et décideurs déterminent le niveau d'appétence de leur organisation pour le risque de sécurité numérique (ou son niveau de tolérance) pour chaque activité qui dépend de l'environnement numérique.

Des **mesures de sécurité** peuvent ensuite être sélectionnées et déployées pour réduire le risque (Principe 7). Ces mesures, appelées aussi « mécanismes », « contrôles » ou « protections », peuvent être de nature diverse : numérique (un logiciel de sécurité, par exemple), physique (des cadenas, caméras, clôtures, etc.) ou hybride (comme une carte à puce) ; s'appliquer aux personnes (une formation, par exemple), aux processus (règles ou pratiques organisationnelles, etc.), ou encore aux technologies (cryptographie) ; être d'ordre juridique (comme un contrat), procédural (normes, par exemple) ou managérial, etc. Les mesures de sécurité peuvent également répondre à des vulnérabilités, conformément à la *Recommandation sur les vulnérabilités* (voir Chapitre 4).

En plus de l'adoption de mesures de sécurité, les parties prenantes peuvent réduire leur exposition au risque de sécurité numérique par l'**innovation**, que celle-ci intéresse l'activité concernée ou les mesures de sécurité (Principe 8). L'innovation en la matière peut revêtir des formes très diverses, touchant ou non

© OCDE 2023

aux aspects numériques. Elle peut, par exemple, avoir trait au modèle économique de l'organisation, à des processus comme ses méthodes de paiement, voire à une nouvelle conception des composantes non numériques, physiques, juridiques ou autres, d'un produit. L'introduction d'une innovation pouvant, en soi, susciter des incertitudes dans une activité, le processus doit donner lieu à un cycle de réévaluation et de traitement du risque, ainsi qu'il ressort du Graphique 3. *La sécurité numérique peut ainsi ajouter de la valeur à une organisation, un produit ou un service, et devenir un moteur d'innovation et de recherche d'avantage comparatif*, pour autant qu'elle soit considérée non comme une question à part et purement technique, mais comme partie intégrante des processus décisionnels économiques et sociaux concernant une activité donnée.

Afin de réduire encore le risque, des **mesures permettant d'assurer la résilience, la préparation et la continuité** peuvent être prédéfinies pour être appliquées en cas d'incident (Principe 9). Outre les mesures de sécurité et l'innovation, dont l'objet est d'empêcher la survenue d'incidents préjudiciables, les mesures de résilience, préparation et continuité de l'activité visent à *atténuer les conséquences économiques et sociales des incidents lorsqu'ils surviennent*. Des plans de préparation et de continuité sont indispensables pour définir à l'avance la manière de se protéger contre ces incidents, de les détecter, d'y répondre et d'assurer la reprise des activités. Ces plans devraient prendre en considération le rythme extrêmement rapide auquel ces incidents peuvent se propager et s'aggraver dans l'environnement numérique.

© OCDE 2023

2. Le niveau stratégique : instaurer une culture de la sécurité numérique

L'élaboration des politiques en matière de sécurité numérique est un exercice multidimensionnel qui nécessite une approche stratégique fondée sur une vision claire afin de faire en sorte que toutes les parties prenantes, des organismes publics aux organisations des secteurs public et privé, en passant par les individus, unissent leurs forces de manière cohérente et homogène. La *Recommandation sur les stratégies nationales* formule des orientations à haut niveau sur les moyens d'atteindre cet objectif et d'instaurer une culture de la sécurité numérique dans l'ensemble de l'économie et de la société.

2.1. Objectifs et cadre institutionnel

Les stratégies nationales de sécurité numérique (appelées ci-après « stratégies nationales ») devraient énoncer une vision claire des objectifs d'un pays en matière de sécurité numérique. Elles devraient viser à insuffler une culture de la sécurité numérique et à protéger les individus ainsi que les organisations privées et publiques des menaces de sécurité numérique tout en tenant compte du besoin de protéger la sécurité nationale et internationale et de préserver les droits de l'homme et les valeurs fondamentales. Les stratégies nationales devraient créer les conditions nécessaires à la gestion, par l'ensemble des parties prenantes, du risque de sécurité numérique, à l'instauration d'un climat de confiance dans l'environnement numérique, au renforcement de la sécurité et de la résilience, et à l'impulsion de la transformation numérique. Elles devraient également avoir pour objet de renforcer la sécurité numérique des activités critiques, thème abordé au Chapitre 3.

En sus de la sécurité numérique, une stratégie nationale peut traiter de plusieurs autres dimensions de la cybersécurité, qui dépassent le cadre du mandat de l'OCDE (voir le point 1.1 et le Graphique 2 plus haut). Il peut arriver que les pouvoirs publics fassent référence à la « cybersécurité » plutôt qu'à la « sécurité numérique », généralement en raison de ces domaines supplémentaires, ou du fait que le terme « cybersécurité » est aujourd'hui très connu du grand public, ou encore parce que le pays se fonde sur une définition de la cybersécurité plus (ou moins) spécifique, qui diffère de celle de l'OCDE. De fait, l'utilisation de ce terme est incohérente dans les différents pays, en particulier à l'échelle internationale. Pour autant, quel que soit l'intitulé retenu, ces stratégies nationales devraient veiller à la cohérence et à la complémentarité entre toutes les dimensions de la cybersécurité.

L'efficacité du cadre institutionnel est une condition essentielle à l'élaboration, la mise en œuvre et l'examen de la stratégie nationale. Il devrait allier coordination intra gouvernementale et processus multipartites. Dans la mesure où la stratégie doit reposer sur une approche à l'échelle de l'ensemble de l'administration, elle doit bénéficier d'un appui des plus hautes instances gouvernementales (le Président ou le Premier ministre, par exemple), afin d'atténuer les difficultés liées aux objectifs concurrents et aux priorités divergentes de différentes composantes de l'administration.

© OCDE 2023

L'établissement d'un dialogue avec le monde des affaires, la communauté technique et la société civile dans le cadre de l'élaboration et de la mise en œuvre de la stratégie est particulièrement important et ne doit pas être considéré comme une simple formalité. Il s'agit tout au contraire d'un outil puissant pour ajuster la stratégie et les politiques de mise en œuvre en fonction de la réalité économique, technique et sociale du pays, et pour éclairer les parties prenantes sur certains aspects des enjeux de la sécurité numérique qu'elles peuvent ignorer. Un dialogue multipartite peut en outre jeter les bases de partenariats fondés sur la confiance (par exemple pour le partage d'informations), qui constituent un élément fondamental d'une stratégie nationale.

La stratégie nationale doit confier des responsabilités claires à au moins un organisme public en place ou nouveau pour l'élaboration et la mise en œuvre des politiques de sécurité numérique préconisées dans la stratégie. Ce ou ces organisme(s) assumant la responsabilité principale de la sécurité numérique devraient néanmoins coordonner leur action avec d'autres organismes compétents dans les domaines de l'application du droit pénal, de la réglementation sectorielle, de la protection de la vie privée et des données, de la protection des consommateurs, de l'innovation, de l'administration numérique, de l'éducation et des affaires étrangères.

Par ailleurs, la stratégie nationale elle-même devrait être cohérente avec d'autres efforts stratégiques nationaux, tels que ceux entrepris dans les domaines des compétences, de l'éducation, de l'innovation et de l'industrie, et les étayer. Comme indiqué plus haut, selon la taille du pays et sa structure institutionnelle, la collaboration avec les organismes publics chargés de ces autres stratégies peut être une tâche ardue du fait de l'existence éventuelle d'obstacles institutionnels ou culturels (OCDE, 2018[25]). Ainsi, les organismes œuvrant dans le domaine de la sécurité nationale ne sont pas toujours accoutumés à collaborer de manière transparente avec les ministères chargés des questions économiques et sociales, ainsi qu'avec des acteurs non gouvernementaux, comme la société civile (voir plus bas).

De nombreux pays ont récemment élaboré des stratégies *numériques* nationales, c'est-à-dire des stratégies globales qui traitent exclusivement ou essentiellement des questions relatives aux politiques du numérique dans les différents domaines d'action qui sont touchés par la transformation numérique ou qui influent sur celle-ci. Dans bien des cas, ces stratégies portent notamment sur la sécurité numérique (Gierten et Lesher, 2022[26]) et leur élaboration offre l'occasion de mettre en évidence les synergies potentielles entre les différentes composantes de l'administration et de renforcer la dimension globale, à l'échelle de l'administration dans son ensemble, des méthodes d'action en matière de sécurité numérique. Les défis liés à la coordination entre les régulateurs sectoriels sont particulièrement aigus lorsqu'il s'agit de la sécurité numérique des activités critiques, ainsi qu'il est expliqué dans le Chapitre 3.

2.2. Contenu de la stratégie

La *Recommandation sur les stratégies nationales* recense neuf domaines dans lesquels les stratégies nationales devraient prévoir des mesures gouvernementales quoique d'autres domaines puissent s'y adjoindre. Aucun ordre de priorité entre ces domaines n'est préconisé dans la Recommandation. Cela dit, de nombreux gouvernements ont généralement débuté avec les trois premiers, à savoir la sensibilisation, la mise en place de capacités de réponse aux incidents (généralement via une équipe de réponse aux incidents de sécurité informatique (CSIRT), également appelée équipe d'intervention en cas d'urgence informatique (CERT)) et la promotion de normes de gestion des risques. À mesure que la sécurité numérique se développe dans un pays, ces domaines doivent être renforcés par des mesures supplémentaires. Pour répondre aux besoins du marché du travail, les pouvoirs publics devraient favoriser le développement et la fidélisation d'une main-d'œuvre qualifiée, notamment en intégrant cette discipline dans les stratégies globales sur les compétences. En sus d'une capacité d'intervention, il est aussi essentiel de mettre en place des mécanismes de coordination de la gestion des vulnérabilités pour favoriser la divulgation coordonnée des vulnérabilités, point abordé plus en détail dans le Chapitre 4. De

© OCDE 2023

plus, les gouvernements devraient encourager les acteurs privés à réagir aux cyberattaques de manière responsable et les dissuader de mener des contre-attaques (voir l'Encadré 1).

Parmi les autres domaines figurent le développement d'une industrie de la cybersécurité, ainsi que des initiatives visant à encourager la recherche et l'innovation (OCDE, 2020[27]), et la protection des individus et des PME (OCDE, 2021[28]). Les stratégies nationales devraient également anticiper les défis croissants en matière de sécurité numérique qui touchent divers secteurs, notamment ceux qui se dotent de systèmes intelligents, comme les transports, l'énergie ou la santé, dans lesquels différents organismes de réglementation peuvent intervenir et où les diverses parties prenantes peuvent avoir des exigences et des besoins différents. Souvent, les ministères et les instances de réglementation sectoriels ne disposent pas encore de la masse critique de compétences nécessaire pour examiner la question de la sécurité numérique et manquent d'une connaissance plus globale du risque à l'échelle mondiale et de la compétence technique que l'on retrouve généralement dans une agence de cybersécurité spécialisée. Des mécanismes de coordination efficaces et une collaboration multipartite sont donc essentiels à la réussite de ces politiques sectorielles.

Afin de mettre en œuvre le principe de coopération énoncé dans la *Recommandation sur la sécurité numérique* (voir le point 1.2), les gouvernements devraient créer les conditions propices à une collaboration de toutes les parties prenantes dans le domaine de la sécurité numérique, en particulier par le biais de partenariats de confiance, notamment pour le partage de l'information liée au risque. Les Centres de partage et d'analyse de l'information (ISAC) constituent un exemple de partenariats multipartites. Parfois mis en place par l'État, qui participe activement ou non à leur gestion, ces centres sont généralement organisés au niveau sectoriel (secteur financier, aviation, énergie, etc.) et peuvent avoir une portée nationale, régionale ou internationale (ENISA, 2018[29] ; CISA, s.d.[30] ; NCSC-NL, 2018[31]). La confiance nécessaire à la coopération entre les parties prenantes est un thème récurrent des recommandations de l'OCDE sur la sécurité numérique. Ce thème est notamment abordé dans le contexte des activités critiques (voir l'Encadré 3) et de la gestion des vulnérabilités (voir le point 4.1). Dernier point, et non des moindres, la coopération internationale devrait occuper une place importante dans les stratégies nationales pour favoriser la mise en commun des expériences et des bonnes pratiques, l'assistance mutuelle, l'amélioration de la réponse aux incidents au niveau opérationnel et l'élaboration d'indicateurs du risque permettant des comparaisons.

Pour la mise en œuvre de leur stratégie nationale en matière de sécurité numérique, les pouvoirs publics devraient allouer des ressources suffisantes et dialoguer avec d'autres parties prenantes. Ils devraient montrer l'exemple, notamment en adoptant les meilleures pratiques en matière de gestion du risque de sécurité numérique afin de protéger les activités de l'administration elle-même. Ils pourraient également recourir aux marchés publics pour promouvoir la gestion du risque de sécurité numérique dans l'ensemble de l'économie et de la société.

Le risque de sécurité numérique est extrêmement volatil, sachant que les menaces et vulnérabilités qui pèsent sur les technologies, les produits et les services utilisés de multiples façons innovantes dans l'économie et la société ne cessent d'évoluer. Dans ce contexte en pleine évolution, les pouvoirs publics doivent formuler, dans les stratégies nationales, des objectifs et des orientations qui restent valables pendant une période suffisamment longue pour que les parties prenantes puissent coordonner leurs actions et avancer dans la même direction. Il ne faudrait toutefois pas que les stratégies nationales soient gravées dans le marbre. Les acteurs malveillants sont connus pour leur agilité et leur aptitude à s'adapter, alors que la sécurité numérique est particulièrement vulnérable aux tensions et aux crises internationales, qui se multiplient dans un monde empreint d'une incertitude croissante. Par conséquent, les pouvoirs publics devraient adopter un cycle d'amélioration en procédant à des évaluations et des révisions régulières et en améliorant leur stratégie et leurs politiques de mise en œuvre.

© OCDE 2023

Encadré 1. Préconiser une réponse responsable et dissuader les contre-attaques (« ripostes numériques »)

Au cours des dernières années, les experts ont observé un essor de la commercialisation clandestine de services de contre-attaque auprès d'acteurs privés, qui peuvent être utilisés pour dissuader les acteurs malveillants de lancer une attaque, endommager leur infrastructure d'attaque ou simplement leur « donner une leçon ».

Ces pratiques, parfois dénommées « ripostes numériques » (*hack back*) sont généralement proposées subrepticement à des entreprises légitimes, dans certains cas par-delà les frontières. Elles sont contre-productives et peuvent sensiblement accroître le risque de dommages collatéraux pour les tierces parties dont les équipements sont utilisés comme intermédiaires par les cybercriminels pour dissimuler leurs activités. Qui plus est, ces pratiques peuvent également accroître le risque d'escalade et exacerber les tensions internationales. Il arrive que les victimes pensent se retourner contre un cybercriminel alors qu'elles ont affaire à un groupe œuvrant pour le compte d'un État, cherchant à atteindre des objectifs politiques ou géopolitiques et doté de ressources quasi illimitées.

La *Recommandation sur les stratégies nationales* stipule que les gouvernements devraient encourager les acteurs privés à réagir aux cyberattaques de manière responsable, les dissuader de mener toute forme de contre-attaque, que ce soit directement ou par l'intermédiaire d'une tierce partie privée, et décourager l'offre ou l'achat de services de contre-attaque par des acteurs privés.

© OCDE 2023

3. Le niveau du marché : renforcer la sécurité sans compromettre la prospérité

Il existe des situations dans lesquelles le seul jeu des forces du marché ne peut permettre à certaines parties prenantes de gérer de manière optimale la sécurité numérique, et dans lesquelles l'action publique est nécessaire pour les inciter à renforcer la sécurité numérique. Cela vaut en particulier pour les activités critiques et pour les produits contenant du code et les services connexes.

Lorsqu'ils gèrent le risque de sécurité numérique, les opérateurs d'activités critiques comme les prestataires de services énergétiques, de télécommunications ou financiers, peuvent avoir pour objectif de réduire le risque au niveau qu'*ils* jugent acceptable, en fonction de *leur* tolérance au risque. Or, leur niveau de risque acceptable peut ne pas correspondre à celui de la société dans son ensemble. Dans la mesure où ils sont responsables d'activités ayant un caractère critique pour le fonctionnement de l'ensemble de l'économie et de la société, le risque résiduel de sécurité numérique que devront inévitablement prendre ces opérateurs (comme cela est expliqué dans la section 1.1) est en partie assumé par tous les autres acteurs économiques et sociaux. Les conséquences d'une défaillance, dans ces cas de figure, vont bien au-delà de ces opérateurs et peuvent être catastrophiques pour tous. Elles peuvent se faire sentir en dehors du secteur directement concerné en raison d'effets en cascade (en cas de cyberattaque contre le réseau électrique provoquant une panne générale qui affecte les transports publics et les hôpitaux, par exemple), et dans d'autres juridictions si l'activité économique touchée se caractérise elle-même par des liens de dépendance internationaux (en cas de cyberattaques paralysant des banques systémiques, par exemple). Il est peu probable que le seul jeu des forces du marché permette de remédier à ce problème. Le rôle et la responsabilité des pouvoirs publics consistent à veiller, par leurs interventions, à ce que les intérêts de l'ensemble de l'économie et de la société soient pris en compte dans la façon dont les opérateurs gèrent le risque de sécurité numérique.

En outre, la plupart des acteurs économiques et sociaux utilisent des produits contenant du code et des services connexes – comme des services de stockage en nuage (*cloud storage*), de traitement, etc. – pour mener à bien leurs activités économiques et sociales. Néanmoins, comment peuvent-ils gérer le risque de sécurité numérique de manière responsable si les produits et services qu'ils utilisent ne sont pas suffisamment sûrs, autrement dit, s'ils n'intègrent pas des dispositifs de sécurité adaptés, tels que des mises à jour de sécurité, tout au long de leur cycle de vie ? Comment les individus et les organisations peuvent-ils prendre des décisions éclairées en matière d'achat de produits et services si le marché ne leur fournit pas suffisamment d'informations sur leur niveau de sécurité ? Là encore, les forces du marché ne semblent pas suffisantes pour garantir que les fournisseurs assument leurs responsabilités selon leur rôle (cf. Principe 2, dans le point 1.2 ci-dessus), et l'action publique peut contribuer à améliorer cette situation.

Dans ces deux domaines, apparemment de natures très différentes, il incombe aux opérateurs d'activités critiques et aux fournisseurs de produits et de services de prendre des décisions relatives au traitement du risque qui peuvent affecter autrui, situation qui est souvent qualifiée d'*aléa moral* et définie comme « toute situation dans laquelle une personne décide de l'ampleur du risque à prendre, tandis que quelqu'un d'autre en supportera le coût si les choses tournent mal » (Krugman, 2009[32]). Ce niveau du Cadre d'action couvre les orientations de l'OCDE destinées à remédier à cet aléa moral afin de renforcer la sécurité

© OCDE 2023

numérique sans compromettre la prospérité, freiner l'innovation, ni réduire les avantages découlant des technologies numériques[12].

3.1. Sécurité numérique des activités critiques

Cette section offre un bref aperçu de la *Recommandation sur les activités critiques* de 2019. La note destinée à la Boîte à outils sur la transformation numérique consacrée au renforcement de la sécurité numérique des activités critiques fournit de plus amples informations et des exemples de politiques publiques dans ce domaine (Bernat, 2021[33]).

Les technologies numériques sont devenues tellement omniprésentes dans les chaînes de valeur et d'approvisionnement que la plupart des activités économiques et sociales sont maintenant tributaires du numérique, et cette dépendance est accentuée et accélérée par la transformation numérique en cours. Parmi ces activités, certaines revêtent une importance cruciale pour la santé, la sûreté et la sécurité des citoyens, le fonctionnement efficace des services essentiels ou, plus globalement, la prospérité économique et sociale (cf. Encadré 2).

Encadré 2. Qu'est-ce qu'une activité critique ?

D'après la *Recommandation sur les activités critiques* de l'OCDE, ce terme désigne les activités économiques et sociales dont l'interruption ou la perturbation aurait de graves conséquences :

- Sur la santé, la sûreté et la sécurité des citoyens (comme les prestations de soins de santé en milieu hospitalier, ou les services d'urgence) ; où
- Sur le fonctionnement efficace des services essentiels à l'économie et à la société (comme les services énergétiques, financiers ou de transport), ainsi que sur celui des pouvoirs publics ; où
- Plus largement, sur la prospérité économique et sociale.

Ce dernier type d'activités critiques recouvre celles qui sont essentielles à la prospérité sans être nécessairement critiques pour le fonctionnement de l'économie et de la société, ni affecter la santé, la sûreté et la sécurité des citoyens. Il inclurait, par exemple, la construction automobile ou le secteur minier dans un pays où ces activités représenteraient une proportion importante du produit intérieur brut (PIB). Les activités critiques sont parfois qualifiées de fonctions critiques ou de services essentiels.

Au cours des dix dernières années, nos économies et nos sociétés sont devenues de plus en plus dépendantes du numérique, et les activités critiques sont de plus en plus exposées aux menaces pesant sur la sécurité numérique, dont le nombre et la sophistication se sont accrus. Cela pousse les pouvoirs publics à changer de vitesse et à adopter des mesures novatrices pour renforcer la sécurité numérique des activités critiques. Néanmoins, un renforcement de la sécurité numérique peut représenter des coûts et d'autres contraintes considérables pour les opérateurs d'activités critiques. Un enjeu clé de l'action publique consiste à veiller à ce que les mesures adoptées *soient axées sur ce qui est critique* pour l'économie et la société, *sans imposer de fardeaux inutiles* par ailleurs, et *sans compromettre les avantages* découlant de la transformation numérique dans les secteurs critiques par des contraintes restreignant inutilement l'usage des technologies numériques et leur ouverture.

La protection des activités critiques n'est pas un nouveau domaine de l'action publique. En 2008, l'OCDE a adopté une *Recommandation sur la protection des infrastructures d'information critiques* (PIIC) (OCDE, 2008[34]), qui était axée sur les réseaux publics de communications, ainsi que sur les systèmes d'information appartenant à des opérateurs d'infrastructures critiques tels que des banques et des

© OCDE 2023

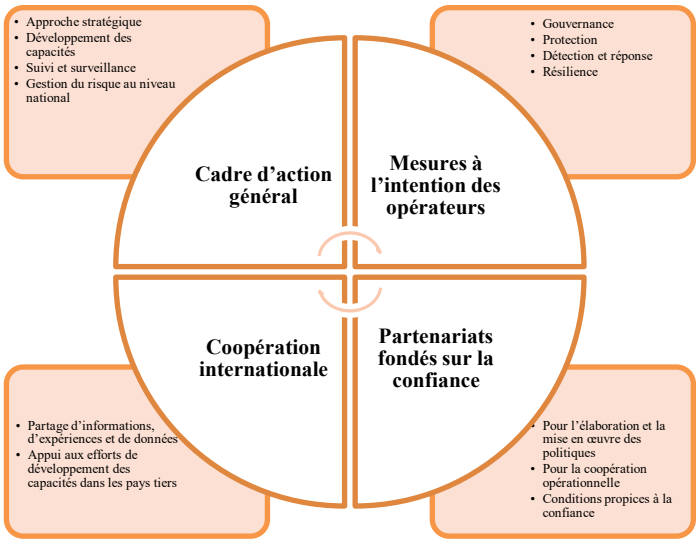
distributeurs d'énergie. Néanmoins, la Recommandation PIIC a été remplacée par la *Recommandation sur les activités critiques* de 2019, qui met l'accent sur le risque de sécurité numérique pesant sur les services économiques et sociaux critiques (activités critiques) plutôt que sur les infrastructures d'information sur lesquelles reposent la fourniture de ces services. Autrement dit, la Recommandation a été réorientée du risque technique vers le risque économique et social, comme indiqué dans la section 1.1.[13]

Les politiques destinées à renforcer la sécurité numérique des activités critiques visent essentiellement à inciter les opérateurs publics et privés de ces activités (dénommés ci-après les « opérateurs ») à mieux gérer le risque de sécurité numérique. On peut citer à titre d'exemple les banques, les hôpitaux, les distributeurs d'eau et d'énergie, les fournisseurs de réseaux de télécommunications, les aéroports, les sociétés de chemin de fer, etc.

Cibler de trop nombreux opérateurs, qui ne sont pas vraiment vitaux pour la réalisation des activités critiques en jeu, imposerait un fardeau inutile à de larges pans de l'économie. À l'inverse, des politiques de portée trop limitée ne protégeraient pas suffisamment l'économie. Pour déterminer quels opérateurs devraient entrer dans le champ d'application de leurs politiques, les pouvoirs publics peuvent s'appuyer sur le cadre existant de protection des infrastructures critiques. En l'absence d'un tel cadre, ils doivent procéder à une évaluation nationale du risque couvrant toutes les activités économiques et sociales, et travailler avec les acteurs publics et privés concernés pour identifier sur cette base les activités critiques ainsi que leurs principaux opérateurs.

Comme le montre le Graphique 4, la *Recommandation sur les activités critiques* offre aux responsables de l'action publique des orientations concernant la définition des mesures que devraient prendre les opérateurs, la mise en place d'un cadre institutionnel adapté, l'établissement de partenariats fondés sur la confiance et la coopération au niveau international,

Graphique 4. Contenu de la Recommandation sur les activités critiques



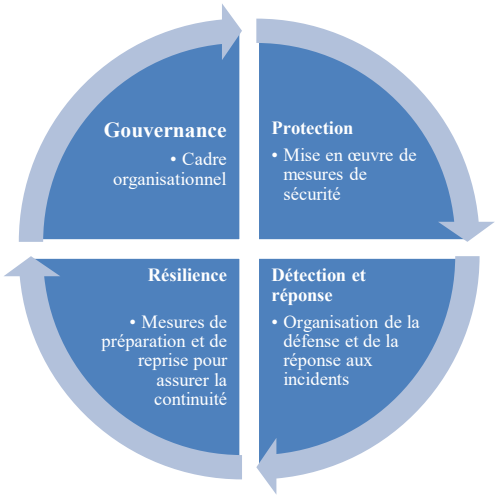
Source : OCDE.

Pour éviter d'imposer des fardeaux inutiles aux opérateurs, les pouvoirs publics devraient axer leurs politiques sur la sécurité numérique des fonctions critiques des opérateurs, qui sont les processus sans lesquels les opérateurs ne pourraient mener à bien efficacement leurs activités critiques. Les pouvoirs

© OCDE 2023

publics peuvent inciter ou contraindre les opérateurs à prendre des mesures en matière de gouvernance, de protection, de détection et de réponse, ainsi que de résilience (cf. Graphique 5). Les autorités peuvent recourir à de nombreux instruments d'action, notamment la promotion de normes, l'instauration d'obligations légales, la réglementation, la Co réglementation, la promotion de l'autoréglementation, l'apport d'une aide à la gestion de crise et d'un soutien technique, etc. La création de partenariats fondés sur la confiance, brièvement présentée dans l'Encadré 3, est un des éléments clés figurant parmi les mesures couvertes par la *Recommandation sur les activités critiques*,

Graphique 5. Types de mesures à l'intention des opérateurs



Source : OCDE.

Encadré 3. Promouvoir des partenariats fondés sur la confiance

La multiplicité des liens de dépendance numérique existant aux niveaux intersectoriel et international et le long des chaînes de valeur des activités critiques crée un risque de sécurité numérique partagé, qui ne saurait être réduit significativement par un seul et unique acteur pour tous. Chaque acteur est donc à la fois dépendant de tous les autres et responsable envers eux en ce qui concerne la gestion du risque de sécurité numérique.

La mise en place de partenariats durables public-public, public-privé et privé-privé, aux niveaux intersectoriel et international, constitue un outil essentiel pour garantir la prise en compte de ces liens de dépendance dans le contexte de la sécurité numérique des activités critiques. Les partenariats de ce type permettent aux participants de partager des informations, des bonnes pratiques et des données d'expérience sur le risque et sa gestion. Ils peuvent également contribuer à améliorer les politiques publiques. Néanmoins, la confiance entre parties prenantes est essentielle à l'émergence de tels partenariats, en partie du fait de la sensibilité des informations à échanger.

La *Recommandation sur les activités critiques* contient une liste de conditions devant être réunies pour instaurer la confiance. Il faut notamment que les objectifs, les valeurs et les règles soient clairement définis, que le partenariat soit mutuellement avantageux au fil du temps, et que soient respectées les règles relatives à la protection des données à caractère personnel et autres dispositions protégeant la

© OCDE 2023

confidentialité des informations telles que les secrets commerciaux. En outre, les partenaires doivent veiller à ce que les informations qu'ils échangent soient utilisées exclusivement à des fins de protection.

3.2. Sécurité numérique des produits et des services

Dans un monde idéal, le jeu des forces du marché permettrait que les produits contenant du code (logiciels, appareils connectés à internet, etc.) et les services connexes soient suffisamment sécurisés, et que leurs mesures de sécurité soient proportionnées au risque qui pèse sur leurs utilisateurs, ce qui se traduirait par une augmentation du coût marginal des cyberattaques pour les acteurs malveillants ayant un effet dissuasif. Des analyses de l'OCDE montrent cependant que des défaillances de marché empêchent souvent les parties prenantes d'estimer de manière optimale la valeur de la sécurité numérique des produits et services, et qu'il est peu probable que les mécanismes d'incitation du marché puissent à eux seuls permettre de combler les lacunes de la gestion du risque de sécurité numérique (OCDE, 2021[35] ; OCDE, 2021[36] ; OCDE, 2021[1]). La complexité et l'opacité des chaînes d'approvisionnement, en particulier, conduisent souvent à une mauvaise répartition des responsabilités en matière de sécurité numérique, et d'importantes *asymétries d'information* empêchent les utilisateurs finaux – notamment les petites et moyennes entreprises (PME) et les consommateurs – de prendre des décisions éclairées quant aux produits et services qu'ils acquièrent. En outre, des *externalités négatives* conduisent souvent les fournisseurs et les utilisateurs des produits à négliger la sécurité numérique, ce qui permet à des acteurs malveillants de les utiliser pour lancer des attaques, y compris à l'échelle internationale. De manière plus générale, le risque de sécurité numérique est mal compris et les mécanismes d'incitation du marché sont inadaptés.

La *Recommandation sur les produits et les services* contient des orientations relatives aux mesures pouvant être adoptées pour réajuster les mécanismes d'incitation du marché et donner aux parties prenantes les moyens d'améliorer la sécurité numérique des produits et des services. Elle met en évidence les domaines dans lesquels les pouvoirs publics devraient intervenir et contient des orientations sur les instruments pouvant être efficaces. Elle couvre les cinq domaines illustrés par le Graphique 6. Cette section ne présente que certains d'entre eux.

La sécurité numérique des produits et des services est bien plus qu'un problème technique nécessitant des solutions techniques. Elle constitue un enjeu essentiel de l'action publique, qui requiert une approche à l'échelle de l'administration dans son ensemble. Les responsables de l'action publique doivent adopter une approche globale de cette question, anticiper au lieu de réagir, et façonner le cadre d'action relatif à la sécurité numérique des produits et des services dans une optique prospective. À cet égard, la coopération internationale apparaît comme une des clés du succès et contribue à favoriser l'interopérabilité des approches nationales, à éviter la prolifération des normes et à limiter les incohérences entre juridictions, qui sont susceptibles de freiner considérablement le développement de l'économie numérique.

© OCDE 2023

Graphique 6. Vue d'ensemble de la Recommandation sur les produits et les services

Coopération

NATIONALE

- Stratégies nationales
- Approche multipartite, à l'échelle de l'administration dans son ensemb
- Développement des capacités pour les utilisateurs vulnérables
- Collaboration et partage d'informations au niveau national (CSIRT/PSIRT/ISAC)

INTERNATIONALE

- Normes et bonnes pratiques internationales
- Partage de bonnes pratiques
- Collaboration et partage d'informations à l'échelle internationale
- Interopérabilité des cadres juridiques
- Développement des capacités dans les pays en développement

Devoir de diligence des fournisseurs

- Sécurité dès la conception et sécurité par défaut
- Gestion et coordination dynamiques des vulnérabilités
- Politiques de fin de support responsables, claires et transparentes
- Coopération entre les propriétaires de code tout au long de la chaîne d'approvisionnement
- Évaluation du niveau de sécurité numérique des produits et des services

Transparence et partage d'informations

- Évaluation par des tierces parties
- Transparence
- Partage d'informations
- Accès et modification par les utilisateurs
- Tests et rétro-ingénierie par les chercheurs de vulnérabilités

Politiques souples

- Écosystème, contexte, usages, appétence pour le risque, maturité…
- Des mesures facultatives aux mesures obligatoires
- Orientations et normes
- Législation relative à la protection des consommateurs et à la responsabilité du fait des produits

Innovation et concurrence

- Marchés concurrentiels
- Programmes de recherche et écosystèmes d'innovation
- Éducation à la sécurité numérique
- Bacs à sable réglementaires
- Marchés publics

Source : OCDE.

Pour réajuster les mécanismes d'incitation du marché, les pouvoirs publics peuvent adopter des mesures visant à garantir que les fournisseurs assument la responsabilité de la sécurité numérique de leurs produits et services tout au long de leur cycle de vie. Ce « *devoir de diligence* » peut être décomposé en 6 lignes d'action pour les fournisseurs :

- *Intégration de la sécurité dès la conception* : les fournisseurs intègrent la sécurité numérique à chaque stade du cycle de vie des produits, en tenant compte du risque de sécurité numérique dans la chaîne d'approvisionnement des produits.
- *Sécurité par défaut* : les fournisseurs assument la responsabilité de la sécurité numérique au lieu de la transférer aux utilisateurs, par exemple en préconfigurant et en activant par défaut les dispositifs de sécurité intégrés aux produits, et en fournissant aux utilisateurs des mises à jour de sécurité jusqu'à la fin du support des produits ;
- *Gestion et coordination continues des vulnérabilités*, conformément aux préconisations de la *Recommandation sur les vulnérabilités* (cf. section 4.1) ;
- *Politiques de fin de support responsables* : les fournisseurs réduisent l'écart entre la fin de support et la fin d'utilisation, par exemple afin d'éviter l'apparition d'un « internet des objets oubliés » ;
- *Coopération entre les responsables de code tout au long de la chaîne d'approvisionnement* : les fournisseurs identifient l'ensemble des éléments de code et des relations de dépendance (nomenclature), et les vulnérabilités sont gérées tout le long de la chaîne d'approvisionnement avec l'aide d'un coordinateur.
- *Évaluation du niveau de sécurité numérique* : les fournisseurs autoévaluent le niveau de sécurité numérique de leurs produits sur la base de normes internationales et/ou font certifier ce niveau dans le cadre d'une évaluation réalisée par une tierce partie.

En outre, pour réduire les asymétries d'information, les pouvoirs publics devraient s'efforcer de *renforcer la transparence et favoriser le partage d'informations* sur la sécurité numérique des produits et des

© OCDE 2023

services. Ce renforcement de la transparence et du partage d'informations vise à sensibiliser les utilisateurs et à leur donner les moyens d'évaluer efficacement le risque de sécurité numérique lié aux produits et aux services, et de prendre des décisions éclairées sur la façon de les utiliser. Il peut aussi inciter les fournisseurs à attacher davantage d'importance à la sécurité numérique de leurs produits et services et à investir dans cette sécurité. Les politiques mises en œuvre dans ce domaine devraient inciter davantage les fournisseurs à communiquer de plus amples informations sur les caractéristiques techniques de leurs produits et services (sur leurs possibilités de mise à jour, par exemple), les processus qu'ils mettent en place (notamment concernant la fin du support) et la traçabilité des composants (au moyen d'une nomenclature, par exemple). La réalisation d'évaluations par des tierces parties (telles que des audits, des tests d'inspection ou des certifications) constitue également une voie prometteuse à explorer pour accroître la transparence.

© OCDE 2023

4. Niveau technique : encourager les bonnes pratiques

Le dernier niveau du Cadre comprend les questions relatives à l'action publique qui sont de nature plus technique. Le traitement des vulnérabilités de sécurité numérique est présenté ci-après (4.1). Les Lignes directrices de l'OCDE régissant la politique de cryptographie (OCDE, 1997[10]) et la Recommandation sur l'authentification électronique (OCDE, 2007[9]) figureront dans une prochaine version.

4.1. Traitement des vulnérabilités

Les vulnérabilités sont des faiblesses susceptibles d'être exploitées pour porter préjudice à des activités économiques et sociales. Elles sont une source majeure de risques de sécurité numérique. Le code informatique, qui constitue le moteur de la transformation numérique, n'est jamais parfait et contient presque toujours des vulnérabilités : là où il y a du code, il y a des vulnérabilités, et plus il y a de code, plus les vulnérabilités sont nombreuses, avec des degrés de gravité variables. De plus, les systèmes d'information présentent également des vulnérabilités liées à la façon dont les logiciels sont mis en œuvre, configurés et mis à jour.

Les criminels et les autres acteurs mal intentionnés cherchent activement à découvrir les vulnérabilités de ces codes et systèmes, et mettent au point ou utilisent des outils (notamment des logiciels malveillants) pour les exploiter en perpétrant des attaques qui portent préjudice à des entreprises, des administrations et des personnes, menacent les activités critiques et sapent la confiance dans l'environnement numérique. Traiter ces vulnérabilités avant que des criminels n'en tirent parti est un moyen efficace de réduire le risque d'incidents.

Les vulnérabilités font partie intégrante de la vie numérique ; elles sont un corollaire de la complexité grandissante du code et des systèmes, alliée aux pratiques de sécurité numérique lacunaires des fournisseurs et des utilisateurs. S'il est impossible d'éliminer entièrement les vulnérabilités du code et des systèmes, l'amélioration de leur gestion permet sans conteste de réduire le risque de sécurité numérique et de renforcer la confiance à l'ère de la transformation numérique.

Pour réduire les risques de sécurité, les parties prenantes devraient, chacune selon son rôle, gérer les vulnérabilités. Les développeurs devraient rechercher et tester les vulnérabilités présentes dans leur code, mettre au point des mesures d'atténuation pour les corriger (par exemple, des correctifs ou des mises à jour de sécurité) et les diffuser auprès d'autres acteurs tout au long de la chaîne de valeur en direction des utilisateurs finaux. Les organisations devraient surveiller leurs systèmes d'information pour s'assurer que ces mesures sont appliquées de manière appropriée et éviter les erreurs de configuration de produit. Ce sont là des tâches complexes et coûteuses, en particulier lorsque les vulnérabilités se situent dans des éléments de code développés par des acteurs tiers de la chaîne logistique, ou dans des logiciels open source, ou affectent de nombreux produits, des organisations sous-dotées, ou des entreprises ayant une faible maturité numérique, à l'instar des acteurs du secteur manufacturier traditionnel se lançant sur le marché de l'internet des objets (IdO). Ces tâches sont également sans fin car les acteurs malveillants

© OCDE 2023

découvrent et exploitent en permanence de nouvelles vulnérabilités. De plus, dans de nombreux cas, les parties prenantes doivent divulguer des informations sur les vulnérabilités qu'elles ont découvertes, par exemple pour faciliter la détection des menaces. La gestion des vulnérabilités est le processus global recouvrant la découverte d'une vulnérabilité et la façon dont la vulnérabilité est traitée par les fournisseurs (les « responsable de code »), administrée par les responsables de systèmes et divulguée au public.

Au cours des dernières années, la communauté technique a progressé dans l'élaboration de bonnes pratiques de gestion des vulnérabilités, notamment grâce à la divulgation coordonnée des vulnérabilités (DCV). Cependant, des difficultés économiques et sociales importantes empêchent les parties prenantes d'adopter des bonnes pratiques. Par exemple, les développeurs logiciels et les responsables de système ont souvent insuffisamment conscience du fait qu'il est de leur responsabilité conjointe de gérer les vulnérabilités. Ils manquent généralement de ressources et de compétences et, parce qu'elles sont décalées, certaines incitations du marché peuvent les décourager de prendre des mesures. Beaucoup d'entre eux sont à même d'ignorer les chercheurs de vulnérabilités, voire de les menacer de poursuites judiciaires. Les chercheurs de vulnérabilité, également dénommés « pirates éthiques », signalent les vulnérabilités aux développeurs logiciels et aux responsables de système qui peuvent ensuite les corriger, ce qui aide à réduire les coûts et la « fenêtre d'exposition » des utilisateurs au risque de sécurité numérique. Quand ils sont ignorés ou menacés, les chercheurs de vulnérabilités peuvent être tentés de divulguer des informations relatives auxdites vulnérabilités sans coordination préalable avec les autres parties prenantes, avec à la clé un risque pour l'ensemble des utilisateurs et pour l'économie. Ils peuvent également se tourner vers le marché noir pour monnayer les informations sur les vulnérabilités, alimentant par là même l'écosystème de la criminalité.

Les politiques publiques visant à supprimer ces obstacles et à encourager la gestion des vulnérabilités ont le potentiel de réduire sensiblement les risques de sécurité numérique pour tous les acteurs (OCDE, 2021[2] ; OCDE, 2021[37] ; OCDE, 2021[38]). Mais la complexité de ce domaine clé est le premier obstacle auquel se heurtent les responsables de l'action gouvernementale lorsqu'ils envisagent de remédier au problème au niveau national. C'est pourquoi, ils doivent d'abord établir un dialogue avec la communauté technique (notamment les chercheurs de vulnérabilités, les responsables de systèmes, les développeurs, les universitaires, etc.) afin de se débarrasser de certaines idées fausses courantes telles que celles que recense l'Encadré 4.

Encadré 4. Idées fausses courantes sur les vulnérabilités de sécurité numérique

La gestion des vulnérabilités est un domaine complexe que les responsables de l'action publique doivent aborder en coopération avec la communauté technique afin d'éviter la mise en place de mesures inefficaces et contre-productives. On trouvera ci-après, recensés sur la base des travaux d'analyse de l'OCDE consacrés aux vulnérabilités, des exemples d'*idées fausses* couramment répandues.

Vous pensez peut-être que...	... alors qu'en réalité
Développer des produits sûrs permet d'éliminer toutes les vulnérabilités et de résoudre le problème.	La sécurité dès la conception est essentielle (cf. 3.2) mais là où il y a du code, il y a toujours des vulnérabilités. Il n'existe aucun produit contenant du code qui soit entièrement sécurisé. Il n'existe pas non plus de remède miracle contre les vulnérabilités et il est impossible de toutes les éliminer, parce que les techniques des cybercriminels évoluent. C'est pourquoi les produits et services nécessitent un suivi constant des vulnérabilités.
La priorité la plus urgente est de mettre au point des solutions d'atténuation (par exemple, des	Mettre au point des solutions d'atténuation pour les failles de type « jour zéro » est essentiel, mais ces solutions sont sans valeur si les responsables de système ne les

© OCDE 2023

correctifs) pour les vulnérabilités du jour zéro, c'est-à-dire les vulnérabilités qui viennent d'être découvertes dans les produits.	mettent pas en œuvre. Le traitement des vulnérabilités est une responsabilité partagée entre les fournisseurs, les responsables de systèmes et les chercheurs de vulnérabilités qui peuvent les aider.
Toutes les mises à jour de sécurité devraient être automatiques, de sorte que les vulnérabilités soient aisément corrigées lorsque des mesures d'atténuation sont disponibles.	Les mises à jour de sécurité elles-mêmes peuvent présenter des risques de sécurité. Les appliquer à l'aveugle à des systèmes complexes, dans de grandes organisations par exemple, peut créer des incidents de sécurité. C'est pourquoi il est fréquent que les responsables de systèmes doivent les tester avant de les appliquer. La gestion des vulnérabilités est un processus fondé sur le risque qui exclut généralement les approches de type universel.
Les pouvoirs publics peuvent aider car ils sont toujours neutres dans ce domaine technique.	Les parties prenantes ne font pas nécessairement confiance aux pouvoirs publics car certains peuvent en réalité acheter des vulnérabilités pour les exploiter. Les pouvoirs publics font partie de la solution, mais aussi du problème. Cela montre que, même si ce domaine est assez technique, nombre d'obstacles sont culturels, sociaux, économiques, juridiques et même politiques.
Les initiatives de type « primes aux bogues » (*bug bounties*), qui consistent pour des organisations à payer des chercheurs pour qu'ils leur signalent les vulnérabilités, sont un moyen de résoudre le problème.	Les « primes aux bogues » peuvent être des outils de grande valeur, mais pas la panacée. Elles conviennent aux organisations matures et dotées à la fois des ressources suffisantes et d'un processus bien rodé de gestion ou de traitement des vulnérabilités. Elles devraient être considérées comme un outil parmi d'autres pour réduire les risques, au même titre que les examens de codes logiciels, les audits et les tests d'intrusion.

Les pouvoirs publics devraient aussi avoir recours à la *Recommandation sur les vulnérabilités* pour asseoir leurs politiques sur des bonnes pratiques internationalement reconnues. La Recommandation se concentre sur cinq domaines d'action (cf. Graphique 7) :

- *Clarifier les responsabilités* de chaque catégorie de parties prenantes, telles que les développeurs et les responsables de systèmes d'information, ou encore les chercheurs de vulnérabilités. Par exemple, les développeurs de logiciels ne devraient pas insérer des vulnérabilités de manière intentionnelle dans leurs produits (« portes dérobées ») ;
- *Instaurer des règles d'exonération et encourager les chercheurs de vulnérabilités*. Les politiques devraient prévoir des règles d'exonération protégeant les chercheurs qui se conforment aux bonnes pratiques contre les menaces de poursuites judiciaires de la part des responsables de la gestion des vulnérabilités, et dissuadant ces derniers de recourir à de telles menaces d'action juridique ;
- *Susciter la confiance*, en veillant à ce que les parties prenantes aient accès à au moins un coordinateur de confiance à même d'aider à résoudre les difficultés entre les participants, et à ce que les chercheurs de vulnérabilités aient confiance dans leurs cadres institutionnels ;
- *Généraliser les bonnes pratiques*, notamment en veillant à ce que les administrations elles-mêmes les mettent en œuvre, en s'appuyant sur les marchés publics, en utilisant la gestion des vulnérabilités comme un indicateur de conformité contractuelle et réglementaire, et en élaborant et diffusant des guides et des manuels sur le sujet ;
- *Intensifier la coopération nationale et internationale* en intégrant la gestion des vulnérabilités à la stratégie nationale en matière de sécurité numérique, en s'appuyant sur la communauté des acteurs de la sécurité, en réduisant le marché gris des vulnérabilités, en favorisant le partage de bonnes pratiques à l'échelle internationale et en veillant à l'interopérabilité internationale des cadres juridiques afin de protéger les chercheurs de vulnérabilités.

Les responsables de l'action publique peuvent aussi utiliser le « Guide de bonnes pratiques sur la coordination de la gestion des vulnérabilités de sécurité numérique » publié par l'OCDE (OCDE, 2022[39])

© OCDE 2023

qui fournit de plus amples informations sur la gestion des vulnérabilités dans la pratique, sans toutefois recourir au jargon technique ni entrer dans des considérations détaillées. Il pourrait également aider les experts techniques en sécurité à communiquer avec les décideurs et les spécialistes non techniques de leur organisation (directeurs, membres du conseil d'administration, services de communication et départements juridiques, etc.) au sujet de la gestion des vulnérabilités.

Graphique 7. Vue d'ensemble de la Recommandation sur les vulnérabilités

Clarifier les responsabilités

- Les propriétaires de code
- Les propriétaires de système adoptent des processus de gestion des vulnérabilités
- Les responsables des vulnérabilités
- Les chercheurs de vulnérabilités assument leur responsabilité, respectent la législation nationale

Instaurer des règles d'exonération et encourager les chercheurs

- Financer la recherche
- Ajuster les cadres juridiques
- Décourager les menaces de recours juridique
- Clarifier la responsabilité juridique des chercheurs de vulnérabilités
- Inciter les responsables de la gestion des vulnérabilités à adopter des politiques de divulgation et éliminer les incohérences avec les conditions de service, les conditions d'utilisation, les licences

Généraliser les bonnes pratiques

- Exemplarité
- Marchés publics
- Gestion des vulnérabilités en tant qu'indicateur de conformité
- Orientations et manuels, modèles et outils
- Normes techniques internationales

Susciter la confiance

- Au moins un coordinateur de confiance pour faciliter la DCV
- Compétence, fiabilité, transparence, prévisibilité des coordinateurs
- Partage de l'information uniquement avec des tiers de confiance
- Coordination transfrontière
- Anonymat
- No misuse of reported vulnerabilities

Intensifier la coopération nationale et internationale

- Intégrer la gestion des vulnérabilités à la stratégie nationale
- Approche multipartite
- Normes internationales
- Partage des bonnes pratiques à l'échelle internationale
- Interopérabilité des cadres juridiques
- Réduction du marché gris

Source : OCDE.

© OCDE 2023

Abréviations

APT – Menaces persistantes avancées

CEI – Commission électrotechnique internationale

CERT – Équipe d'intervention en cas d'urgence informatique

CISA – *Cybersecurity and Infrastructure Security Agency*

CRE – Conduite responsable des entreprises

CSIRT – Équipe de réponse aux incidents de sécurité informatique

DCV – Divulgation coordonnée de vulnérabilités

ENISA – Agence de l'Union européenne pour la cybersécurité

EMN – Entreprises multinationales

IA – Intelligence artificielle

IdO – Internet des objets

IETF – *Internet Engineering Task Force*

ISAC – Centre de partage et d'analyse de l'information

ISO – Organisation internationale de normalisation

NCSC – *National Cyber Security Centre*

NIST – *National Institute of Standards and Technologies*

OCDE – Organisation de coopération et de développement économiques

OEWG – Groupe de travail à composition non limitée

ONG – Organisation non gouvernementale

ONUDC – Office des Nations Unies contre la drogue et le crime

PIIC – Protection des infrastructures d'information critiques

TIC – Technologies de l'information et des communications

UIT-T – Union Internationale des Télécommunications, Secteur de la normalisation

UNGGE – Groupe d'experts gouvernementaux des Nations Unies

© OCDE 2023

Références

Bernat, L. (2021), *Enhancing the digital security of critical activities*, OECD Going Digital Toolkit Notes, No. 17, OECD Publishing, Paris, https://doi.org/10.1787/a91b818b-en. [33]

CISA (s.d.), *Information Sharing and Analysis Organizations (ISAOs)*, https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos. [30]

ENISA (2018), *Information Sharing and Analysis Center (ISACs) - Cooperative models*, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models. [29]

Gierten, D. et M. Lesher (2022), *Assessing National Digital Strategies and their Governance*, OECD Digital Economy Papers, No. 324, OECD Publishing, Paris, https://doi.org/10.1787/baffceca-en. [26]

Krugman, P. (2009), *The Return of Depression Economics and the Crisis of 2008*, W. W. Norton & Company. [32]

NCSC-NL (2018), *Starting an ISAC: Sectoral Collaboration. Guide*, https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2019/juli/02/ncsc-guide-isac/ncsc_guide_isac.pdf. [31]

NIST (2018), *Cybersecurity Framework*, https://www.nist.gov/cyberframework. [3]

OCDE (2022), *Guide de bonnes pratiques sur la coordination de la gestion des vulnérabilités de sécurité numérique*, OCDE, Paris, https://one.oecd.org/document/DSTI/CDEP/SDE(2021)9/FINAL/FR. [39]

OCDE (2022), *Recommandation du Conseil sur la gestion des vulnérabilités de sécurité numérique*, OECD/LEGAL/0482, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0482. [8]

OCDE (2022), *Recommandation du Conseil sur la gestion du risque de sécurité numérique*, OECD/LEGAL/0479, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0479. [4]

© OCDE 2023

OCDE (2022), *Recommandation du Conseil sur la sécurité numérique des produits et des services*, OECD/LEGAL/0481, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0481. [7]

OCDE (2022), *Recommandation du Conseil sur les stratégies nationales de sécurité numérique*, OECD/LEGAL/0480, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0480. [5]

OCDE (2021), *Encourager le traitement des vulnérabilités*, OCDE, Paris, https://www.oecd.org/fr/numerique/encourager-le-traitement-des-vulnerabilites.pdf. [37]

OCDE (2021), *Des politiques intelligentes pour les produits intelligents*, OCDE, Paris, https://www.oecd.org/fr/numerique/politiques-intelligentes-produits-intelligents.pdf. [1]

OCDE (2021), « Digital security in SMEs », dans *The Digital Transformation of SMEs*, Éditions OCDE, Paris, https://doi.org/10.1787/cb2796c7-en. [28]

OCDE (2021), « Encouraging vulnerability treatment : Overview for policy makers », *Documents de travail de l'OCDE sur l'économie numérique*, n° 307, Éditions OCDE, Paris, https://doi.org/10.1787/0e2615ba-en. [2]

OCDE (2021), *Encouraging vulnerability treatment: background report - Responsible management, handling and disclosure of vulnerabilities*, OCDE, Paris, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf. [38]

OCDE (2021), « Enhancing the digital security of products: A policy discussion », *OECD Digital Economy Papers*, n° 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en. [36]

OCDE (2021), *Recommandation du Conseil sur la connectivité à haut débit*, OECD/LEGAL/0322, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0322. [14]

OCDE (2021), *Recommandation du Conseil sur les enfants dans l'environnement numérique*, OECD/LEGAL/0389, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0389. [16]

OCDE (2021), « Understanding the digital security of products: An in-depth analysis », *OECD Digital Economy Papers*, n° 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en. [35]

OCDE (2020), « Encouraging digital security innovation: Global Forum on Digital Security for Prosperity », *Documents de travail de l'OCDE sur l'économie numérique*, n° 298, Éditions OCDE, Paris, https://doi.org/10.1787/e65d02af-en. [27]

OCDE (2020), « Going Digital integrated policy framework », *Documents de travail de l'OCDE sur l'économie numérique*, n° 292, Éditions OCDE, Paris, https://doi.org/10.1787/dc930adc-en. [11]

© OCDE 2023

OCDE (2019), « Policies for the protection of critical information infrastructure : Ten years later », *Documents de travail de l'OCDE sur l'économie numérique*, n° 275, Éditions OCDE, Paris, https://doi.org/10.1787/efb55c54-en. [40]

OCDE (2019), *Recommandation du Conseil sur l'intelligence artificielle*, OECD/LEGAL/0449, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449. [15]

OCDE (2019), *Recommandation du Conseil sur la sécurité numérique des activités critiques*, OECD/LEGAL/0456, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0456. [6]

OCDE (2018), « Digital security policy », dans *OECD Reviews of Digital Transformation : Going Digital in Sweden*, Éditions OCDE, Paris, https://doi.org/10.1787/9789264302259-6-en. [25]

OCDE (2018), *Guide OCDE sur le devoir de diligence pour une conduite responsable des entreprises*, https://www.oecd.org/fr/daf/inv/mne/Guide-OCDE-sur-le-devoir-de-diligence-pour-une-conduite-responsable-des-entreprises.pdf. [18]

OCDE (2018), *Recommandation du Conseil relative au Guide de l'OCDE sur le devoir de diligence pour une conduite responsable des entreprises*, OECD/LEGAL(0443), OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0443. [41]

OCDE (2016), *Déclaration sur l'économie numérique : innovation, croissance et prospérité sociale (Déclaration de Cancún)*, OECD/LEGAL/0426, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0426. [21]

OCDE (2016), *Recommandation du Conseil sur la protection du consommateur dans le contexte du commerce électronique*, OECD/LEGAL/0422, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0422. [13]

OCDE (2015), *Principes de gouvernance d'entreprise du G20 et de l'OCDE*, Éditions OCDE, Paris, https://doi.org/10.1787/9789264269514-fr. [20]

OCDE (2015), *Recommandation du Conseil relative aux Principes de gouvernance d'entreprise*, OECD/LEGAL/0413, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0413. [19]

OCDE (2013), *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OECD/LEG/0188, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188. [12]

OCDE (2011), *Déclaration sur l'investissement international et les entreprises multinationales*, OECD/LEGAL/0144, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0144. [17]

© OCDE 2023

OCDE (2011), *Les principes directeurs de l'OCDE à l'intention des entreprises multinationales, édition 2011*, Éditions OCDE, Paris, https://doi.org/10.1787/9789264115439-fr. [24]

OCDE (2011), *Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet*, OECD/LEGAL/0387, Paris, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0387. [22]

OCDE (2008), *Déclaration sur le futur de l'économie Internet (La Déclaration de Séoul)*, OECD/LEGAL/0366, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0366. [23]

OCDE (2008), *Recommandation du Conseil sur la protection des infrastructures d'information critiques*, OECD/LEGAL(0361), OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0361. [34]

OCDE (2007), *Recommandation du Conseil sur l'authentification électronique*, OECD/LEGAL/0353, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0353. [9]

OCDE (1997), *Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie*, OECD/LEGAL/0289, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0289. [10]

© OCDE 2023

Notes

[1] Toutes les recommandations de l'OCDE sont disponibles dans le Recueil en ligne des instruments juridiques de l'OCDE.

[2] Disponibles à l'adresse : https://oe.cd/securite.

[3] Cf. Principe 3. (« Droits humains et valeurs fondamentales ») de la Recommandation sur la sécurité numérique.

[4] Voir également www.oecd.org/fr/gouvernementdentreprise/mne/ et (OCDE, 2011[24]), pour consulter une édition commentée des Principes directeurs EMN.

[5] Le Guide sur le devoir de diligence est évoqué dans la Recommandation relative au Guide de l'OCDE sur le devoir de diligence pour une conduite responsable des entreprises (OCDE, 2018[41]).

[6] Du strict point de vue de la gestion des risques, le risque est l'effet de l'incertitude sur les objectifs. Cet effet peut être préjudiciable ou bénéfique.

[7] Les normes ISO/IEC définissent le risque comme l'« effet de l'incertitude sur les objectifs ». Lorsque les parties prenantes évaluent le risque, l'incertitude est généralement caractérisée en termes de *probabilité* et l'effet en termes de *gravité*.

[8] Cf. ISO/IEC Guide 73:2009 « Management du risque – Vocabulaire », et ISO/IEC 27000:2018 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire ».

[9] www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf.

[10] Outre le texte intégral de la Recommandation, le *Document d'accompagnement de la Recommandation du Conseil de l'OCDE sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale* de 2015 fournit des explications supplémentaires sur ces principes.

[11] Aux termes des Principes directeurs EMN, les entreprises devraient « 10. Exercer une diligence raisonnable fondée sur les risques, par exemple en intégrant cette dimension dans leurs systèmes de gestion des risques, afin d'identifier, de prévenir ou d'atténuer les incidences négatives, réelles ou potentielles [...]. 11. Éviter d'avoir, du fait de leurs propres activités, des incidences négatives dans des domaines visés par les Principes directeurs, ou d'y contribuer, et prendre des mesures qu'imposent ces incidences lorsqu'elles se produisent. 12. S'efforcer d'empêcher ou d'atténuer une incidence négative, dans le cas

© OCDE 2023

où elles n'y ont pas contribué mais où cette incidence est néanmoins directement liée à leurs activités, à leurs produits ou à leurs services en vertu d'une relation d'affaires. » (Chapitre II. Principes généraux, section A) (OCDE, 2011[24]).

[12] Il peut exister d'autres domaines, non couverts actuellement par le Cadre d'action, dans lesquels une intervention des pouvoirs publics pourrait être nécessaire pour remédier à d'autres défaillances du marché.

[13] La logique de cette évolution est exposée de manière plus précise dans (Bernat, 2021[33]) et (OCDE, 2019[40]).

© OCDE 2023