OECD Note sur les politiques STI

www.oecd.org/fr/sti

Encourager le traitement des vulnérabilités

Comment les politiques publiques peuvent-elles aider à pallier les vulnérabilités de sécurité numérique ?

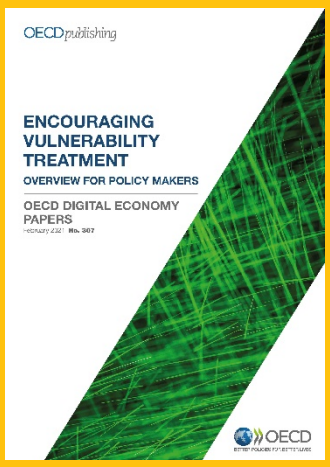
Le risque de cyber sécurité sape la confiance dans la transformation numérique et induit des coûts économiques et sociaux importants. Selon les estimations, les incidents de sécurité numérique coûtent entre 100 milliards USD et 6 000 milliards USD par an. Le risque de cyber sécurité constitue également une menace de plus en plus sérieuse pour la sécurité des individus, alors qu'un nombre croissant de consommateurs et d'entreprises ont recours à des dispositifs d'internet des objets (IdO) vulnérables.

La plupart des incidents de sécurité numérique sont le fait d'acteurs malveillants (par exemple, des cybercriminels ou des groupes soutenus par des États) qui exploitent les vulnérabilités dans les écosystèmes numériques des organisations. Traiter ces vulnérabilités avant que ces acteurs malveillants n'en tirent parti est un moyen efficace de réduire la probabilité d'incidents.

Les vulnérabilités sont des failles qui peuvent être exploitées pour porter atteinte aux activités économiques et sociales. Elles constituent une source importante de risque de sécurité numérique. Le code informatique, moteur de la transformation numérique, n'est jamais parfait et présente presque toujours des vulnérabilités. Les systèmes d'information comportent des vulnérabilités liées à l'implémentation, la configuration et la mise à jour des logiciels. Les criminels et autres acteurs ayant l'intention de nuire tentent de découvrir ces vulnérabilités, et développent ou utilisent des outils tels que les logiciels malveillants (ou « maliciels ») qu'ils utilisent pour attaquer des entreprises, des administrations et des individus, menaçant ainsi les activités critiques, et sapant la confiance dans la transformation numérique.

En bref

Pour réussir la transformation numérique, il est essentiel de traiter les vulnérabilités dans le code des produits et celles créées lors de l'implémentation des systèmes d'information. Ces dernières années, la communauté technique a élaboré des bonnes pratiques en matière de traitement des vulnérabilités, notamment s'agissant de la divulgation coordonnée des vulnérabilités (CVD). Pour autant, d'importants obstacles économiques et sociaux empêchent les parties prenantes d'adopter ces bonnes pratiques, tels le manque de sensibilisation et de coopération, des incitations limitées ou contradictoires, des obstacles juridiques ainsi que des ressources et des compétences insuffisantes.



Les pouvoirs publics doivent prendre des mesures pour faire évoluer les mentalités à l'égard des vulnérabilités, encourager l'adoption de bonnes pratiques et lever les obstacles tels que les cadres juridiques imparfaits qui font peser des risques sur les chercheurs en sécurité.

Cette note résume les principales conclusions des travaux de l'OCDE sur ce sujet, exposées dans OCDE, 2021a et 2021b.

Pour réduire le risque de cyber sécurité, les développeurs devraient donc tester leur code à la recherche de vulnérabilités, mettre au point des correctifs pour y remédier et distribuer ces correctifs aux autres acteurs de la chaîne de valeur, jusqu'aux utilisateurs finaux. Les organisations devraient également surveiller leurs systèmes d'information afin de s'assurer que les correctifs ont été correctement installés et d'éviter les mauvaises configurations des produits. Ces opérations sont complexes, lourdes et coûteuses. Elles sont également sans fin, car les acteurs malveillants découvrent et exploitent continuellement de nouvelles vulnérabilités. Fort heureusement, les chercheurs en sécurité peuvent détecter les vulnérabilités et les signaler aux organisations. Également connus sous le nom de « pirates éthiques » (ou « *hackers* éthiques »), ces chercheurs sont désireux de contribuer à la réduction du risque et de faciliter l'adoption de bonnes pratiques, bien que de nombreux obstacles empêchent de tirer profit de leur expertise. Comme l'a montré une analyse récente de l'OCDE, des politiques publiques visant à lever ces obstacles et à encourager le traitement des vulnérabilités peuvent réduire considérablement le risque de sécurité numérique pour l'ensemble des acteurs (OCDE, 2021a, b).

Pour réussir la transformation numérique, il faut traiter efficacement les vulnérabilités

Toutes les vulnérabilités ne sont pas équivalentes

Les acteurs malveillants qui exploitent les vulnérabilités de sécurité numérique peuvent avoir des objectifs variés: voler de l'argent, des données personnelles, des secrets commerciaux ou des secrets d'État, perturber les activités commerciales et/ou demander une rançon à des parties prenantes, comme des entreprises, des villes et des hôpitaux. L'OCDE a examiné dans quelle mesure les politiques publiques peuvent aider à relever les défis posés par les vulnérabilités du code des produits (*vulnérabilités de code*) et les vulnérabilités liées à la façon dont les produits sont implémentés dans les systèmes d'information des organisations (*vulnérabilités des systèmes*), en laissant de côté d'autres formes de vulnérabilité, comme les défaillances humaines.

Le code contenu dans les logiciels et le matériel informatique (i.e. microprogrammes) contient presque toujours des vulnérabilités dont le degré de gravité et de risque est variable. *Les vulnérabilités de code* peuvent être atténuées si les concepteurs des produits mettent au point des correctifs et les distribuent par le biais de mises à jour de sécurité. Les *vulnérabilités du jour zéro* (ou « zero day ») sont des vulnérabilités de code pour lesquelles aucun correctif n'a encore été diffusé. Elles attirent particulièrement l'attention des médias car il est très difficile pour les utilisateurs des produits de les détecter et d'en atténuer les effets. Les incidents du jour zéro ont généralement un grand retentissement. L'attaque Stuxnet de 2010, qui a partiellement détruit une installation d'enrichissement nucléaire iranienne, et l'attaque de 2016 contre le Comité national démocrate des États-Unis, en sont des exemples.

Cependant, les cybercriminels n'utilisent pas souvent des vulnérabilités du jour zéro, car elles sont difficiles à découvrir, coûtent cher sur les marchés noir et gris (voir ci-après) et perdent de la valeur dès qu'elles ont été détectées. La plupart des attaques exploitent plutôt les *vulnérabilités des systèmes*, qui comprennent les failles liées à l'implémentation ou à la configuration des produits au sein des systèmes d'information. Le défaut d'installation des dernières mises à jour de sécurité représente une source majeure de vulnérabilités des systèmes, de même que les erreurs de configuration. Les attaques de type WannaCry et NotPetya, qui ont causé des milliards de dollars de dommages au niveau mondial, ou encore les incidents qui ont frappé Equifax (1.4 milliard USD de dégâts) ou ont entraîné une panne générale d'électricité en Ukraine en 2016, étaient tous fondés sur des vulnérabilités de systèmes. Dans une enquête réalisée en 2019 auprès de professionnels des technologies de l'information, 60 % des personnes interrogées ont déclaré qu'une ou plusieurs des atteintes dont ils avaient été la cible s'étaient produites parce qu'un correctif mis à disposition pour gérer une vulnérabilité connue n'avait pas été appliqué[1].

Le traitement des vulnérabilités de code et des systèmes est essentiel pour réduire les risques et accroître la confiance

Les vulnérabilités font partie de la vie numérique. Elles sont le corollaire de la complexité croissante du code et des systèmes, conjuguée à des lacunes dans les pratiques de sécurité numérique des concepteurs et des utilisateurs. S'il est impossible d'éradiquer totalement les vulnérabilités du code et des systèmes, l'amélioration de leur traitement offre une possibilité importante de réduire le risque de sécurité numérique et de renforcer la confiance dans la transformation numérique.

Le traitement des vulnérabilités comprend leur détection, leur résolution, leur gestion et leur divulgation publique. Une fois les vulnérabilités identifiées (détection), les responsables du code doivent les corriger en mettant au point et en distribuant des correctifs ou d'autres mesures d'atténuation (résolution). Il incombe ensuite aux

responsables des systèmes d'appliquer ces correctifs (gestion). Enfin, les vulnérabilités doivent généralement être divulguées publiquement afin d'enrichir les connaissances en matière de sécurité et de faciliter la protection.

Les « responsables de vulnérabilités », c'est-à-dire les personnes à qui appartient la responsabilité de les traiter, sont donc :

- *Les responsables du code*, c'est-à-dire les développeurs des produits qui comportent du code (biens, services ou produits hybrides, commercialisés ou disponibles gratuitement, propriétaires ou libres). Ils devraient non seulement rendre leur code aussi robuste que possible, mais aussi assurer un devoir de diligence : détecter et résoudre les vulnérabilités de leurs produits dès leur mise à la disposition des utilisateurs ; et
- *Les responsables des systèmes*, à savoir les organisations qui utilisent des produits dans les systèmes d'information soutenant leurs activités économiques et sociales. Ils devraient détecter et gérer les vulnérabilités afin de protéger ces activités ainsi que l'ensemble des tiers auxquels des incidents pourraient porter préjudice.

À l'ère de la transformation numérique, il serait irresponsable de développer du code et de maintenir des systèmes tout en ignorant les conséquences des vulnérabilités qui peuvent apparaître au fil du temps. Les concepteurs de produits et les responsables de systèmes d'information doivent mettre en place des processus pour traiter les vulnérabilités de façon systématique et proactive, de manière à réduire le risque pour eux-mêmes et pour autrui, ainsi que pour la société dans son ensemble.

D'importants défis économiques et sociaux empêchent les parties prenantes de traiter efficacement les vulnérabilités

Le traitement des vulnérabilités est une question autant économique et sociale que technique

Le traitement des vulnérabilités pose des défis liés au manque de sensibilisation et de coopération entre les parties prenantes, aux incitations de marché limitées ou contradictoires, aux obstacles juridiques, ou encore à l'insuffisance des ressources et des compétences. Le traitement des vulnérabilités peut être complexe, en particulier lorsque les vulnérabilités concernent du code élaboré par un tiers ou touchent un grand nombre de produits. Cette combinaison de coûts, temps et complexité accrus peut s'avérer insurmontable pour les petites et moyennes entreprises (PME), les organismes du secteur public et les organisations ayant une faible maturité numérique, à l'instar des fabricants traditionnels qui s'implantent sur les marchés de l'IdO grand public ou industriel. Sans compter que le traitement des vulnérabilités est une course contre la montre, les acteurs malveillants s'efforçant en permanence de trouver et d'exploiter les vulnérabilités existantes et nouvelles.

Le traitement des vulnérabilités est un processus délicat basé sur la gestion du risque

Pour mener à bien leur mission, les « responsables de vulnérabilités » doivent évaluer le risque associé à chaque vulnérabilité dont ils ont connaissance, de manière à identifier celles auxquelles ils doivent consacrer en priorité leurs efforts et leurs ressources.

Les responsables du code doivent décider du correctif à mettre au point en priorité. La difficulté de cette tâche réside en partie dans le fait que le risque associé à une vulnérabilité du code dépend du contexte d'utilisation du produit, qui varie considérablement d'un utilisateur à l'autre et n'est pas nécessairement connu du responsable du code.

Il est également difficile pour les responsables de système de hiérarchiser les correctifs à implémenter, car ils ont besoin de comprendre le risque qu'implique l'application de chaque correctif à leur système. Or, ce risque peut être élevé. Si l'application silencieuse et automatique de correctifs est un objectif raisonnable pour les produits grand public, il n'en va pas de même pour des systèmes d'information plus complexes utilisés par les organisations. Nombre d'entre elles doivent souvent tester les mises à jour de sécurité avant de les appliquer, afin d'évaluer si le correctif lui-même va perturber les activités opérationnelles ou introduire par effet domino des problèmes de compatibilité, de performance ou d'instabilité. En 2020, l'attaque SolarWinds, qui atteint l'administration américaine et des entreprises privées via leur chaîne d'approvisionnement, a montré que des acteurs malveillants peuvent également perpétrer des attaques de sécurité en compromettant des dispositifs de mise à jour. Selon les enquêtes, il faut en moyenne 102 jours aux organisations pour tester et déployer pleinement les correctifs ; les délais vont de 16 jours pour corriger une vulnérabilité critique à 151 jours pour corriger une vulnérabilité de priorité moyenne ou faible[2].

Les chercheurs en cyber sécurité constituent une ressource importante mais sous-exploitée

Les chercheurs en sécurité sont des individus ou des organisations qui identifient des vulnérabilités du code ou d'un système dans le but de réduire le risque de sécurité. Les médias les dénomment souvent « chapeaux blancs » (*white hats*) ou « pirates informatiques éthiques » (*ethical hackers*), bien que « pirate informatique » soit un terme ambigu, car à connotation négative. Ces chercheurs sont animés par des objectifs divers et soumis à des contraintes différentes. Nombre d'entre eux recherchent des vulnérabilités dans le cadre de leurs activités professionnelles au sein d'universités, d'entreprises de sécurité numérique, d'équipes de sécurité au sein de fournisseurs de produits, d'organismes publics ou de la société civile. Pour d'autres il s'agit d'un passe-temps.

En pratique, les chercheurs en sécurité aident les « responsables de vulnérabilités » à déceler et à divulguer les vulnérabilités qui les concernent avant que des acteurs malveillants ne les exploitent. Pourtant, ils ne sont souvent pas accueillis favorablement car nombre de responsables de vulnérabilités se sentent menacés par les signalements des chercheurs plutôt qu'aidés dans le traitement des vulnérabilités, et/ou n'ont pas une connaissance suffisante des bonnes pratiques dans ce domaine.

Les chercheurs en sécurité sont trop souvent exposés à des poursuites judiciaires

Dans de nombreux pays, il arrive souvent qu'au lieu de les accueillir favorablement, des responsables de vulnérabilités menacent de poursuites judiciaires les chercheurs en sécurité qui leur signalent des vulnérabilités dans leur produit ou système d'information. Ce faisant, ils peuvent invoquer le droit pénal, le droit de la propriété intellectuelle, le droit applicable en matière de protection des données personnelles et le droit des contrats. Ce risque juridique, aggravé lorsque les parties prenantes se trouvent dans des pays différents, exerce un puissant effet dissuasif, voire paralysant, au sein de la communauté de la sécurité numérique. Il varie selon que le cadre juridique du pays ou territoire du responsable de la vulnérabilité a été conçu ou non pour protéger les chercheurs en sécurité. La culture du responsable de la vulnérabilité et son niveau de sensibilisation aux bonnes pratiques en la matière, ainsi que le comportement du chercheur lorsqu'il signale une vulnérabilité, sont également des facteurs importants.

Exemples de chercheurs exposés à des poursuites judiciaires

En 2011, la plateforme de jeux en ligne finlandaise Habbo (273 millions d'utilisateurs dans 150 pays) a engagé des poursuites pénales contre un adolescent qui avait indiqué comment il pouvait se connecter au service d'assistance technique du site. Deux ans plus tard, les tribunaux ont prononcé un non-lieu.

En 2013, des chercheurs de l'Université de Radboud (Pays-Bas) ont informé un fabricant de puces de vulnérabilités dans l'un de leurs produits largement utilisée dans les dispositifs antidémarrage de différentes marques de voitures. La même année, un tribunal britannique, agissant à la demande de Volkswagen, a statué que l'article scientifique détaillant la vulnérabilité devait être retiré. Deux ans plus tard, Volkswagen a finalement accepté la publication de l'article.

En 2015, un chercheur en sécurité a signalé une vulnérabilité à l'éditeur d'une application de vote électronique en Argentine qui allait être utilisée pour des élections la semaine suivante. Trois jours avant les élections, la police a perquisitionné son appartement et saisi son matériel informatique en se fondant sur la plainte l'entreprise. L'affaire a été classée sans suite un an plus tard au motif qu'il n'avait pas pénétré illégalement dans les systèmes de l'entreprise ni causé de préjudice.

En 2016, des chercheurs ont reçu une lettre de mise en demeure trois jours après avoir signalé une importante vulnérabilité à l'entreprise internationale de conseil et d'audit PwC. Un autre chercheur a fait l'objet d'une perquisition à son domicile et a été arrêté par le FBI après avoir signalé qu'un fabricant de logiciels de soins dentaires n'avait pas crypté des informations médicales sensibles de 22 000 patients auxquelles n'importe qui pouvait avoir accès.

En 2017, un citoyen danois a détecté une vulnérabilité sur le site web d'une municipalité qui permettait de collecter les données à caractère personnel de tout citoyen en saisissant sa date de naissance dans un formulaire. Il a signalé cette vulnérabilité à la municipalité. Le prestataire de services a discrètement corrigé la vulnérabilité et a dénoncé le chercheur à la police.

En 2020, les chercheurs du MIT ont détecté dans le système de vote électronique de l'entreprise Voatz des vulnérabilités pouvant permettre à des pirates de modifier, de bloquer ou de dévoiler le vote d'un utilisateur individuel. L'application avait déjà été utilisée aux États-Unis lors de plusieurs élections au niveau local et des États. Ayant noté l'attitude négative de Voatz à l'égard d'un étudiant qui avait recherché des vulnérabilités en 2018 et que l'entreprise avait dénoncé au FBI, les chercheurs du MIT ont fait part de leurs conclusions à la *Cybersecurity and Infrastructure Security Agency* (CISA). L'entreprise a contesté la gravité des vulnérabilités, faisant des déclarations publiques agressives à l'encontre des chercheurs. Finalement, un audit indépendant commandité par Voatz a confirmé les conclusions du MIT.

Sources : OCDE (2021a), « Encouraging vulnerability treatment: Overview for policy makers », https://doi.org/10.1787/0e2615ba-en ; OCDE (2021b), « Encouraging vulnerability treatment: Background report – Responsible management, handling and disclosure of vulnerabilities ».

La divulgation coordonnée des vulnérabilités (CVD) est une bonne pratique essentielle encore insuffisamment adoptée

Lors d'un processus de CVD, responsables de vulnérabilités et chercheurs travaillent de concert pour découvrir des vulnérabilités, développer, diffuser et appliquer les correctifs qui permettent de les corriger, et divulguer largement les informations sur ces vulnérabilités sans donner aux cybercriminels un avantage chronologique. Toutefois, le recours à de tels processus peut s'avérer complexe, en particulier lorsque la coordination implique de nombreuses parties prenantes, comme dans les cas où la vulnérabilité est localisée dans un composant présent dans de nombreux produits. En outre, chaque découverte d'une vulnérabilité est différente, et la CVD peut être inadaptée ou impossible dans certains cas.

Les parties prenantes peuvent utiliser plusieurs outils pour faciliter la CVD et, plus généralement, le traitement des vulnérabilités :

- Une **politique de divulgation des vulnérabilités** est une déclaration publique par laquelle un responsable de vulnérabilité invite les chercheurs à lui signaler des vulnérabilités, leur donnant l'assurance que leurs signalements seront traités avec sérieux, et réduisant le risque d'action en justice lorsque cette politique est à la fois bien conçue et respectée par le chercheur.
- Un **coordinateur** peut apporter son aide en tant que tiers de confiance dans divers cas, qu'il s'agisse de simplifier et faciliter les relations entre les parties prenantes, y compris par-delà les frontières, ou de mettre en place une coordination multipartite complexe. Par exemple, certaines équipes d'intervention en cas d'urgence informatique (CERT) et de réponse aux incidents de sécurité informatique (CSIRT) jouent également un rôle de coordinateur en matière de vulnérabilités. Tel est le cas du CERT/CC de l'Université Carnegie Mellon, du Centre national de cybersécurité des Pays-Bas (NCSC-NL), de la CISA du département de la Sécurité intérieure des États-Unis et, en France, de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information.
- Les **normes et bonnes pratiques** permettent aux parties prenantes d'avoir une compréhension commune des processus et des procédures de coordination du traitement, de la résolution et de la divulgation des vulnérabilités.
- Dans le cadre des **programmes de « prime aux bogues »** (« *bug bounties* »), les responsables de vulnérabilités récompensent les chercheurs qui leur signalent des vulnérabilités sous certaines conditions prédéfinies. Plusieurs plateformes en ligne facilitent l'organisation de tels programmes en offrant un marché pour les responsables de vulnérabilités et les chercheurs.

Les parties prenantes n'ont souvent pas confiance dans les pouvoirs publics

Dans certains cas, les forces de l'ordre et les administrations en charge du renseignement ou de la sécurité nationale recherchent des vulnérabilités en vue de les exploiter à leurs propres fins. Les politiques publiques permettent souvent à ces services de découvrir des vulnérabilités sans les signaler aux organisations ayant la responsabilité de les corriger. Ces services peuvent accumuler ces vulnérabilités, puis en faire des armes qu'ils exploitent contre des cibles publiques ou privées. Ces services peuvent également acheter des vulnérabilités pour mener à bien des « opérations offensives ». Il arrive que les pouvoirs publics exigent des développeurs qu'ils intègrent dans leurs produits des « portes dérobées », qui équivalent à des vulnérabilités intentionnelles. Cette pratique est condamnée par d'autres parties prenantes et par certains gouvernements. L'ambiguïté de la position des pouvoirs publics concernant l'exploitation des vulnérabilités peut compromettre l'efficacité des politiques visant à promouvoir le

traitement des vulnérabilités en sapant la confiance des autres parties prenantes dans les efforts déployés par ailleurs par les pouvoirs publics pour réduire les risques.

Le marché gris des vulnérabilités de code peut rendre l'attaque plus attrayante que la défense

Idéalement, toutes les vulnérabilités de code découvertes par des acteurs non légitimes devraient faire l'objet d'un signalement aux responsables de la vulnérabilité, qui élaboreraient alors un correctif que tous les utilisateurs des produits seraient chargés d'appliquer, réduisant ainsi les risques. Cependant, d'autres acteurs sont prêts à acheter des vulnérabilités de code critiques à des prix élevés, sans l'intention de les corriger. Parmi ces acteurs figurent des criminels qui achètent des vulnérabilités sur le marché noir, mais aussi des organismes publics chargés du renseignement et de la défense, ainsi que des entreprises qui développent et commercialisent des outils basés sur l'exploitation des vulnérabilités, comme ceux achetés par les services de police ou de renseignement pour accéder au contenu des téléphones portables. De nombreux experts estiment que ce marché gris peut détourner les chercheurs de leur mission de signalement auprès des responsables de vulnérabilités, et rendre l'attaque plus rentable que la protection.

Les décideurs peuvent jouer un rôle décisif

Le traitement des vulnérabilités mérite une plus grande attention de la part des pouvoirs publics

Jusqu'à présent, le traitement des vulnérabilités n'a pas fait l'objet d'une attention suffisante de la part des pouvoirs publics. Bien que la transformation numérique offre des avantages considérables, elle repose aussi sur des milliards de dispositifs IdO potentiellement vulnérables et sur des systèmes d'information complexes exécutant cumulativement des centaines de milliards de lignes de code. Alors que des criminels et d'autres types d'attaquants saisissent toutes les occasions de nuire, comme on le voit depuis le début de la pandémie de COVID-19, les efforts déployés par les pouvoirs publics pour encourager les parties prenantes à traiter plus efficacement les vulnérabilités ont été limités.

Les pouvoirs publics peuvent prendre des mesures dans de nombreux domaines

Pour encourager le traitement des vulnérabilités et réduire le risque de sécurité numérique, les politiques publiques peuvent:

- ***Faire évoluer la culture et les mentalités*** en brisant le « tabou des vulnérabilités » et en reconnaissant que les vulnérabilités font « partie de la vie numérique » et peuvent être atténuées en adoptant des bonnes pratiques. Trop souvent, les dirigeants des organisations tiennent pour acquis que leurs produits et/ou systèmes sont « sûrs et sécurisés », et considèrent les vulnérabilités comme une défaillance qui portera atteinte à leur réputation et sapera la confiance de leurs partenaires. Or ils doivent comprendre que tous les produits comprenant du code contiennent aussi des vulnérabilités, et que tous les systèmes d'information ont une forte probabilité de présenter des vulnérabilités liées à des erreurs de configuration ou à des logiciels – y compris des microprogrammes – non mis à jour. À l'ère du numérique, les dirigeants et les décideurs doivent :
  - abandonner l'idée d'un environnement numérique parfaitement sécurisé
  - reconnaître que leurs produits et leurs systèmes d'information peuvent être vulnérables
  - instaurer la confiance en montrant qu'ils assument leurs responsabilités par rapport aux vulnérabilités, grâce à un effort continu pour les traiter, couvrant à la fois leur détection, leur résolution et leur gestion rapides ainsi que leur divulgation.
- **Généraliser les bonnes pratiques.** Pour ce faire, les pouvoirs publics peuvent :
  - *Donner l'exemple.* Les pouvoirs publics peuvent adopter des pratiques de divulgation coordonnée des vulnérabilités, ainsi que de résolution et de gestion des vulnérabilités auxquelles ils sont eux-mêmes confrontés. Par exemple, aux États-Unis, l'Agence en charge de la Sécurité des Infrastructures et de la Cybersécurité (CISA) a publié une directive opérationnelle contraignante (BOD 20-01) exigeant que chaque agence fédérale adopte et publie une politique de divulgation des vulnérabilités. Par ailleurs, plusieurs gouvernements ont lancé des programmes de « *bug bounty* » (voir Encadré ci-dessous). Ils peuvent également se servir de la commande publique pour promouvoir un changement de culture en matière de traitement des vulnérabilités.
  - *Inclure le traitement des vulnérabilités dans la réglementation, les normes et les orientations*, ou l'utiliser comme indicateur de conformité. Les gouvernements peuvent utiliser la réglementation des produits, la réglementation relative aux activités critiques, comme la directive NIS de l'UE (actuellement en cours de

révision), les dispositifs de certification, comme ceux établis par le règlement sur la cybersécurité de l'UE, les normes soutenues par les pouvoirs publics (par exemple, le *Cybersecurity Framework* du NIST, ou la spécification technique de l'ETSI intitulée *Cyber Security for Consumer Internet of Things* (cybersécurité relative à l'internet des objets grand public)), la réglementation de l'IdO (par exemple, le projet de règlement du Royaume-Uni), ou encore la réglementation relative à la protection de la vie privée (par exemple, le Règlement général sur la protection des données de l'UE et la loi américaine connue sous le nom de *Health Insurance Portability and Accountability Act*).

  - *Fournir des outils et encourager l'élaboration et l'adoption de normes*. Tous les groupes de parties prenantes peuvent faciliter l'adoption de la divulgation coordonnée des vulnérabilités grâce à des modèles de politiques en la matière, des guides et d'autres documents relatifs aux bonnes pratiques. Le modèle sur la divulgation coordonnée des vulnérabilités « au stade préliminaire » de la NTIA Américaine destiné aux activités critiques et les lignes directrices du NCSC-NL sur la divulgation coordonnée des vulnérabilités sont des exemples de telles initiatives. Les travaux récents de l'OCDE offrent un aperçu de haut niveau des bonnes pratiques en la matière, fondées sur les orientations existantes (OCDE, 2021a, b).

- **Renforcer la confiance et lever les obstacles**. Pour ce faire, les pouvoirs publics peuvent :
  - *Faciliter l'accès à un coordinateur de confiance,* qui peut aider à mettre en relation les parties prenantes en cas de besoin et fournir des analyses et un appui techniques supplémentaires. Les coordinateurs doivent disposer de ressources suffisantes pour accomplir leur mission, qui peut être exigeante. Il n'est pas nécessaire que chaque pays dispose d'un coordinateur national. Par exemple, les parties prenantes peuvent se tourner vers un coordinateur de confiance étranger, régional, international ou au niveau de l'industrie.
  - *Mettre à jour les cadres juridiques en matière de cybercriminalité et de propriété intellectuelle pour permettre l'établissement de « zones de protection » pour les chercheurs*. Les décideurs de politiques publiques doivent modifier l'environnement juridique pour mieux protéger les chercheurs en sécurité responsables et réduire le risque de litiges et de poursuites judiciaires chaque fois que ce risque fait obstacle à la divulgation coordonnée des vulnérabilités. Les pouvoirs publics peuvent faire le bilan du risque juridique qui pèse sur les chercheurs dans leur pays ou sur leur territoire, élaborer un plan pour l'atténuer et veiller à ce que tout nouveau cadre législatif ou réglementaire ne crée pas de nouveaux obstacles.
  - *Renforcer la confiance des parties prenantes dans les pouvoirs publics*, par exemple en s'assurant que les organismes en charge de la sécurité numérique et les CERT n'assurent pas de fonctions offensives, et en fixant des processus transparents encadrant la manière dont les pouvoirs publics traitent les informations sur les vulnérabilités.
  - *S'attaquer au marché gris des vulnérabilités de code*. Si certains acteurs légitimes doivent légalement pouvoir acheter des vulnérabilités, les pouvoirs publics doivent prendre des mesures pour garantir que ces transactions ne découragent pas les chercheurs de signaler les vulnérabilités en faussant les prix, et n'empêchent pas les responsables de vulnérabilités d'élaborer des mesures d'atténuation et de protéger les utilisateurs. Des travaux de recherche supplémentaires sont nécessaires pour mieux comprendre la dimension et les mécanismes de fixation des prix sur le marché gris et les moyens de réduire son impact négatif sur la divulgation des vulnérabilités, ainsi que les mesures d'incitation et de dissuasion qui pourraient être utilisées pour modifier les comportements des acteurs.
- **Encourager la coopération internationale,** notamment par la mise en place d'un coordinateur international non gouvernemental, l'internationalisation des bases de données sur les vulnérabilités, l'élaboration de principes communs visant à établir des zones de protection pour les chercheurs et la définition de normes et de bonnes pratiques internationales.

Au moment de prendre des mesures, les décideurs doivent garder à l'esprit que :

- **Il n'existe pas de solution unique concernant la divulgation des vulnérabilités.** Il s'agit d'un problème épineux sans remède miracle, qui nécessite une ouverture d'esprit, des solutions flexibles et un examen au cas par cas, souvent sur la base de normes et de lignes directrices internationales ;
- **Les pouvoirs publics devraient recourir à la réglementation contraignante avec prudence**. Par exemple, l'obligation de signaler les vulnérabilités aux pouvoirs publics est particulièrement problématique, et de nombreux experts suggèrent l'adoption d'une approche volontaire fondée sur la confiance mutuelle.

Qu'est-ce qu'un programme de *bug bounty* ?

Les programmes de *bug bounties*, ou de « primes aux bogues », ou encore « chasses aux vulnérabilités », sont des initiatives participatives menées par des responsables de vulnérabilités pour récompenser les personnes qui découvrent et signalent des vulnérabilités dans le cadre d'un processus de CVD. En plus d'aider à trouver les vulnérabilités, ces programmes peuvent motiver le personnel interne à mieux prendre en compte la sécurité, et contribuer à maintenir un niveau élevé de sensibilisation à cet égard. Ils peuvent également servir d'outil de recrutement, en facilitant l'identification des talents et en aidant les chercheurs en sécurité à sélectionner les entreprises répondant à leurs attentes en matière d'emploi. Du point de vue des politiques publiques, ils peuvent contribuer à purger le marché noir en offrant une alternative aux chercheurs motivés par une rémunération financière, à condition qu'ils soient mis en place uniquement sous l'autorité de responsables de vulnérabilités, et non de courtiers du marché gris.

Les *bug bounties* recueillent peu à peu l'adhésion de nombreuses entreprises de renom, notamment les grands acteurs du secteur des technologies de l'information et des communications (TIC), tels Apple, Google, ou Microsoft, d'autres entreprises numériques et de communication (Airbnb, Alibaba, AT&T, Deezer, Deutsche Telekom, Facebook, Nintendo, OVH, Samsung, Twitter, Uber, par exemple) et des entreprises traditionnelles (Audi, Fiat Chrysler, Ford, Goldman Sachs, Mastercard, Starbucks, etc.). Les plateformes de *bug bounty* peuvent, quant à elles, faciliter l'organisation de tels programmes.

Les pouvoirs publics lancent également des chasses aux vulnérabilités. Par exemple, le Département de la Défense des États-Unis y a consacré 34 millions USD en 2018, suite au succès de ses précédentes initiatives « *Hack the Pentagon* » (Pirater le Pentagone) et « *Hack the Army* » (Pirater l'Armée). À Singapour, deux organismes publics (GovTech et CSA) ont distribué en 2018-19 un total de 26 000 USD de primes à 290 chercheurs dans le cadre de *bug bounties* ciblant les systèmes publics. En 2019, le gouvernement suisse a offert 150 000 USD pour la découverte de vulnérabilités dans son système de vote électronique sur internet, avec des récompenses allant de 100 à 50 000 USD. En 2020, il a également lancé un *bug bounty* pour son système de traçage de proximité appelé « SwissCovid ». Le gouvernement français a lancé un *bug bounty* pour son application de messagerie instantanée Tchap à usage des fonctionnaires, avec des primes allant de 50 à 1 500 USD. Le ministère coréen de la Science et des TIC et l'Agence coréenne de sécurité de l'information (KISA) ont mis en place un *bug bounty* axé sur les sites web d'entreprises privées volontaires ainsi que sur celui de KISA.

Cependant, les *bug bounties* ne sont ni une panacée ni une solution de sécurité clé en main. Ils conviennent aux organisations dotées de ressources et d'une maturité suffisantes, et qui disposent déjà d'un processus bien organisé de résolution et de gestion des vulnérabilités. En outre, il s'agit de mesures réactives qui, seules, ne sont pas à même d'améliorer les problèmes de sécurité inhérents à la conception d'un produit ou d'une ligne de produits. Les chasses aux vulnérabilités devraient par conséquent être utilisées comme un outil parmi d'autres pour réduire le risque, au même titre que les examens du code informatique, les audits de sécurité et les tests d'intrusion dans les réseaux.

Sources : OCDE (2021a), « Encouraging vulnerability treatment: Overview for policy makers », https://doi.org/10.1787/0e2615ba-en ; OCDE (2021b), « Encouraging vulnerability treatment: Background report – Responsible management, handling and disclosure of vulnerabilities » ; www.bugcrowd.com/bug-bounty-list/.

Notes

1 Ponemon Institute (2019), *Costs and consequences of gaps in vulnerability response*, https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.

2 Ponemon Institute (2019), et Ponemon Institute (2018), *The 2018 State of Endpoint Security Risk*, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf.

Pour aller plus loin

OCDE (2021a), « 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/10.1787/20716826.

OCDE (2021b), *Encouraging Vulnerability Treatment: Background Report - Responsible Management, Handling and Disclosure of Vulnerabilities*, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf.

Site web

https://oe.cd/securite

Note sur les politiques de la Direction de la science, de la technologie et de l'innovation

Cette série de Notes sur les politiques a été conçue pour mettre à la disposition d'un public plus large certaines des études destinées à un usage interne à l'OCDE.

Les commentaires sur cette Note sur les politiques sont les bienvenus et peuvent être adressés à l'OCDE, 2 rue André Pascal, 75775 Paris Cedex 16, France, ou par courriel à l'adresse : digitalsecurity@oecd.org.

Merci de citer cette note comme suit :

OCDE (2021), « Encourager le traitement des vulnérabilités », *Note sur les politiques de la Direction de la science, de la technologie et de l'innovation*, Éditions OCDE, Paris, www.oecd.org/fr/numerique/encourager-le-traitement-des-vulnerabilites.pdf.

Pour rester au fait de l'actualité STI, abonnez-vous à la lettre d'information : **OECD News on Innovation, Science, Technology and Industry**, http://www.oecd.org/fr/sti/news.htm.

@OECDInnovation

http://oe.cd/securite

Contact : STI.contact@oecd.org.