CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE SUR LES POLITIQUES DE DIVULGATION COORDONNEE DE VULNERABILITES

PARTIE I : BONNES PRATIQUES

COORDINATED VULNERABILITY DISCLOSURE POLICIES -"CVDP"
RESPONSIBLE DISCLOSURE POLICIES -"RD"

CENTRE POUR LA CYBERSECURITE BELGIQUE
Rue de la Loi, 16
1000 Bruxelles

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. TABLE DES MATIERES

CENTRE FOR CYBER SECURITY BELGIUM

<u>Avertissement</u> :

Le présent guide vise à exposer les concepts, les objectifs, les questions juridiques et les bonnes pratiques liées à l'adoption de politiques de divulgation coordonnée de vulnérabilités (ou Coordinated Vulnerability Disclosure Policies – « CVDP ») dans l'état actuel de la législation en Belgique – voir les exemples fournis sur le site du CCB.

L'attention des lecteurs est attirée sur le fait que les documents élaborés par le CCB ne constituent nullement une modification des règles légales existantes. L'accès non autorisé au système informatique d'un tiers, même avec de bonnes intentions est une infraction pénale.

Le participant à une CVDP doit être conscient qu'il ne bénéficie pas d'une exclusion générale de responsabilité lorsqu'il participe à une telle politique : il doit agir avec précaution et respecter scrupuleusement toutes les conditions de la politique, ainsi que les dispositions légales applicables.

** Shutterstock - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

B. INTRODUCTION

I. Contexte

L'importance croissante des systèmes d'information au sein de nos sociétés augmente considérablement le risque d'être confronté à des incidents liés à la sécurité de ceux-ci. Ces incidents peuvent, par exemple, avoir pour conséquence d'affecter la disponibilité d'un service fourni, l'intégrité, l'authenticité, ou la confidentialité de données. L'usage grandissant d'objets connectés à internet accroît encore plus les conséquences éventuelles d'un incident.

Parmi les causes de ces incidents, l'existence de vulnérabilités constitue un risque majeur. Celui-ci est toutefois inhérent au processus de développement, d'utilisation et de mise à jour de ces systèmes. Compte tenu de l'ampleur et de la technicité de ce problème, il apparaît illusoire de croire que tous les fabricants ou responsables de systèmes d'information pourront être en mesure d'y remédier seuls.

Une organisation peut choisir de faire appel soit à une entreprise particulière pour vérifier la sécurité de ses systèmes d'information (via un audit de sécurité par exemple), soit de manière publique à des personnes bien intentionnées (« *hackers éthiques* ») qui souhaitent contribuer à l'amélioration de la sécurité de ces technologies en identifiant les vulnérabilités existantes et en aidant à les résoudre.

II. Notions

A. *Une politique de divulgation coordonnée de vulnérabilités*[1] *(CVDP)* est un ensemble de règles préalablement déterminées par une organisation responsable de systèmes d'information autorisant des participants[2] (ou « *hackers éthiques* ») à rechercher, avec de bonnes intentions, de potentielles vulnérabilités dans ses systèmes, ou à lui transmettre toute information pertinente à ce sujet. Ces

[1] Dénommé également « politique de divulgation responsable » : le choix du terme divulgation « coordonnée » plutôt que « responsable » nous paraît préférable dans la mesure où il évite toute confusion avec les notions légales de responsabilité et il insiste sur le caractère réciproque du processus.

[2] Il peut s'agir, par exemple, de chercheurs en cybersécurité ou des utilisateurs. Les participants peuvent éventuellement être soumis à une sélection par un tiers de confiance (« coordinateur »).

règles, généralement rendues publiques sur un site internet, permettent de fixer un cadre juridique à la collaboration entre l'organisation responsable et les participants à la politique. Elles doivent notamment assurer la confidentialité des informations échangées et encadrer, de manière responsable et coordonnée, une éventuelle divulgation des vulnérabilités découvertes.

Ainsi, la notion de « divulgation » ne doit pas être comprise comme impliquant nécessairement une communication publique de la vulnérabilité mais plutôt une communication du participant vers l'organisation responsable. Si la divulgation de la vulnérabilité par le participant à l'organisation responsable est obligatoire, la divulgation publique de la vulnérabilité (par le participant ou l'organisation concernée) est, en revanche, facultative dans le cadre d'une CVDP.

B. ***Une vulnérabilité*** [3] est un défaut ou une faiblesse, une erreur de conception[4] ou de mise en œuvre[5], une absence de mise à jour au regard des connaissances techniques actuelles et qui peut compromettre la sécurité de technologies[6] de l'information. Une vulnérabilité peut conduire potentiellement à un événement inattendu ou indésirable, et être exploitée par des tiers malveillants en vue de violer l'intégrité, l'authenticité, la confidentialité, la disponibilité d'un système[7] ou d'endommager.

[3] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, p. 14, point 2.2, www.enisa.europa.eu/publications/vulnerability-disclosure.

[4] Par exemple, une erreur ou un oubli dans la conception d'un système ou d'un protocole qui le rendent intrinsèquement vulnérable.

[5] Par exemple, une erreur au cours de l'implémentation, de la configuration ou de l'exploitation.

[6] Par exemple, un système, un réseau, un procédé, un programme, une application, un service, un protocole ou un composant.

[7] ou des informations qu'il contient.

C. ***Une organisation responsable*** est une personne physique ou morale, gestionnaire, propriétaire, vendeur ou fabricant, d'un système ou d'un produit liés aux technologies de l'information et qui est, à ce titre, responsable de la sécurité et du bon fonctionnement de celui-ci.

D. ***Le participant à une CVDP[8] (ou « hacker éthique »)*** est une personne bien intentionnée qui souhaite contribuer, avec l'autorisation de l'organisation responsable, à l'amélioration de la sécurité de systèmes d'information. Celui-ci peut, par exemple, réaliser des tests d'intrusion ou utiliser d'autres méthodes pour vérifier la sécurité de systèmes d'information. Il s'oppose au *hacker* qui utilise ses compétences pour tenter d'accéder à un système sans autorisation et avec de mauvaises intentions[9]. Le participant entend quant à lui avertir le responsable du système d'information, ou un coordinateur, des éventuelles vulnérabilités découvertes afin de les éliminer.

E. ***Un coordinateur*** est un personne physique ou morale qui sert d'intermédiaire entre le participant et l'organisation responsable d'un système d'information en fournissant une assistance logistique, technique et juridique, ou encore d'autres fonctions[10], afin de faciliter leur collaboration. A défaut de coordinateur désigné dans la politique, ce rôle peut être joué par le Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be).

F. ***Un programme de récompense pour la découverte de vulnérabilités (*ou *bug bounty)[11]*** vise l'ensemble des règles définies par une organisation responsable pour octroyer des récompenses aux participants qui identifieraient des vulnérabilités dans les technologies qu'elle utilise. Cette récompense peut prendre la forme d'une somme d'argent, de cadeaux ou d'une reconnaissance publique (classement parmi les meilleurs participants, publication, conférence, etc.). Il s'agit d'une forme de politique de divulgation coordonnée de vulnérabilités, qui prévoit l'octroi d'une récompense

[8]communément dénommé en anglais «white hat », par référence au fait que les héros dans les films de western américains portaient traditionnellement un chapeau blanc.
[9] Communément dénommé en anglais « black hat », par référence au fait que les bandits dans les films de western américains portaient traditionnellement un chapeau noir.
[10] Par exemple, un rôle d'évaluateur des rapports de vulnérabilités ou de médiateur.
[11] En anglais, « vulnerability rewards program » ou « bug bounty program ».

pour le participant, en fonction du nombre, de l'importance ou de la qualité des informations transmises. Cette forme de politique est plus attrayante pour les éventuels participants et offre souvent de meilleurs résultats pour les organisations. L'organisation peut notamment faire appel à une plate-forme de *bug bounty* qui lui offre une assistance technique et administrative pour la gestion de son programme de récompense pour la découverte de vulnérabilités (rôle de coordinateur).

III. Objectifs

a. Offrir un cadre juridique permettant une collaboration utile, loyale, efficace, légale et à budget maîtrisé

Lorsqu'une organisation fait appel à un prestataire externe déterminé pour vérifier la sécurité de ses systèmes d'information, elle conclut avec lui un contrat d'audit de sécurité qui peut inclure la réalisation de tests d'intrusion (en anglais : *penetration test* ou « *pentest* ») simulant l'attaque de personnes mal intentionnées en vue de démontrer les vulnérabilités existantes. Dans ce cas, les obligations juridiques réciproques des parties sont, en principe, définies dans une convention particulière ou des conditions générales[12].

Cela n'est toutefois pas le cas, par défaut, lorsqu'une organisation souhaite collaborer avec des personnes indéterminées (*participant*s ou *hackers éthiques*) qui seraient susceptibles d'identifier des vulnérabilités dans ses systèmes d'information. Il n'existe alors pas de cadre contractuel précis entre les parties. Dans ce cas de figure, il s'avère nécessaire pour l'organisation de fixer préalablement à toute collaboration ses attentes et les obligations juridiques des participants.

La politique de divulgation coordonnée de vulnérabilités constitue, à ce titre, une forme de contrat d'adhésion dans lequel toutes les dispositions contractuelles sont fixées par l'organisation responsable

[12] L'organisation responsable pourrait également confier ces tâches à certains de ses employés. Les obligations respectives des parties seront alors définies par un règlement interne spécifique ou dans le règlement général de travail.

et ensuite acceptées par le participant lorsque celui-ci décide librement de participer au programme mis en place.

L'adoption d'une telle politique clarifie la situation juridique des participants en leur permettant de prouver, moyennant le respect des conditions énoncées dans la politique, l'existence d'une autorisation préalable d'accès aux systèmes informatiques concernés et dès lors l'absence d'une intrusion illicite (*voir Guide sur les politiques de divulgation coordonnée de vulnérabilités. Partie II : Aspects légaux*).

Cette collaboration peut procurer de manière loyale et licite à l'organisation responsable des informations sur les vulnérabilités de ses systèmes, en lui permettant d'agir de manière appropriée et en temps opportun. Celle-ci permet ainsi de prévenir efficacement ou de limiter, dans la mesure du possible, les risques et les dommages potentiels que pourraient lui causer ces vulnérabilités.

La politique de divulgation coordonnée de vulnérabilités offre la possibilité de vérifier de manière constante et efficace la sécurité de ses systèmes ou équipements. Bien entendu, l'attractivité et l'efficacité de la politique sont augmentées lorsque l'organisation responsable décide d'accorder des récompenses aux participants en fonction de l'importance et de la qualité des informations fournies (dans le cadre d'un programme de récompense pour la découverte de vulnérabilités ou *bug bounty*[13]).

Même lorsque l'organisation octroie des récompenses et fait appel à un coordinateur externe (plate-forme de *hacking éthique*), les coûts liés à la mise en place d'une politique de divulgation coordonnée de vulnérabilités sont, en général, mieux maîtrisés que ceux liés à la réalisation d'audits par des entreprises externes[14]. En effet, l'octroi d'une récompense dans le cadre d'un bug bounty résulte d'une obligation de résultat dans le chef du participant alors que l'auditeur externe n'est généralement tenu

[13] En dehors d'un programme de récompense pour la découverte de vulnérabilités, l'organisation responsable peut unilatéralement décider d'accorder une récompense (non prévue) au participant à l'issue de la procédure.
[14] Certains coûts sont nécessairement à prévoir, comme par exemple, le coût de l'équipe technique nécessaire à l'analyse des informations fournies par les participants.

qu'à une obligation de moyens. Ce dernier devrait ainsi être rémunéré pour l'ensemble de ses prestations même s'il ne trouve pas de vulnérabilités ou des vulnérabilités mineures à l'issue de ses recherches.

b. Augmenter la sécurité des systèmes d'information et encourager les recherches

En adoptant une politique, l'organisation responsable se donne l'opportunité de recevoir de plusieurs sources des informations sur la sécurité de ses systèmes d'information. Compte tenu de la complexité et de la technicité actuelles de tels systèmes, il s'avère très utile de recourir à une multitude d'experts potentiels plutôt que de faire appel à quelques prestataires externes qui peuvent difficilement être experts dans toutes les technologies utilisées par l'organisation.

En complément à d'autres mesures techniques et organisationnelles, la mise en place d'une telle collaboration peut constituer une mesure appropriée en vue de prévenir les incidents qui compromettraient la sécurité de ses réseaux et systèmes d'information. Elle présente l'avantage indéniable d'identifier les vulnérabilités et d'y remédier avant qu'un incident de sécurité ne se produise.

L'amélioration de la sécurité découle de la correction des vulnérabilités, de la minimisation des risques lié à l'existence de vulnérabilités et d'un processus constant d'évaluation de ces mêmes risques pour les systèmes d'information de l'organisation responsable.

Bien entendu, l'adoption d'une CVDP implique que l'organisation dispose de mesures de sécurité qui puissent être mises à l'épreuve et d'une équipe interne (ou externe) capable d'assurer un suivi des informations reçues des participants.

Outre l'amélioration de la sécurité, de telles politiques peuvent également améliorer les connaissances en matière de cybersécurité et encourager les recherches dans ce domaine. Or, les travaux des

chercheurs permettent d'identifier les nouvelles vulnérabilités, les conditions dans lesquelles elles se produisent, les méthodes pour les éviter et les moyens de les corriger.

c. Assurer la confiance des utilisateurs dans les technologies de l'information

La mise en œuvre d'une CVDP témoigne vis-à-vis du public et des utilisateurs de l'attachement de l'organisation responsable à la sécurité de ses technologies de l'information.

En effet, cette démarche implique l'engagement de traiter les informations fournies par les participants et d'essayer de remédier aux vulnérabilités identifiées, ou à tout le moins d'informer les utilisateurs des risques encourus.

Cet engagement peut par ailleurs constituer un argument marketing et être mis en avant dans la communication de l'organisation. La confiance dans les systèmes d'information est assurément un élément important pour les utilisateurs ou les consommateurs.

d. Garantir la confidentialité

La confidentialité des informations liées à une vulnérabilité dans un système informatique doit être assurée autant que possible.

La divulgation complète d'une vulnérabilité[15], alors que celle-ci existe toujours auprès de nombreux utilisateurs, constitue un risque important de sécurité en matière de technologies de l'information. En

[15] « full disclosure ».

effet, des tiers malveillants pourraient développer et répandre des outils spécifiques pour exploiter cette vulnérabilité.

Il n'est donc pas souhaitable qu'une faille de sécurité soit divulguée au public, avant qu'elle n'ait été corrigée par l'organisation responsable, en lui accordant le temps nécessaire à la résolution du problème, ou avant que l'organisation responsable n'ait pu en informer préalablement les autorités publiques en charge de la sécurité des réseaux et systèmes d'information[16].

La divulgation complète est également susceptible de retarder le déploiement efficace d'une solution à la vulnérabilité en imposant à l'organisation responsable de réagir en situation de crise.

De même, la révélation publique de failles de sécurité peut porter atteinte à la réputation de l'organisation responsable et entamer la confiance des utilisateurs dans les technologies concernées.

En outre, le fait de diffuser ou de mettre à disposition du public des données informatiques, tels que des logiciels ou des instructions, adaptées pour forcer la sécurité de systèmes informatiques peut constituer une infraction[17] ou engager la responsabilité civile de celui qui a publié les informations[18] (*voir Guide – partie II Aspects légaux*).

Par voie de conséquence, la divulgation publique d'informations sur une vulnérabilité doit être réalisée avec beaucoup de précaution et de manière coordonnée avec l'organisation responsable.

---

[16] En Belgique, ce rôle est principalement joué par le Centre pour la Cybersécurité Belgique (CCB) qui peut, le cas échéant, informer les organisations d'intérêt vital (autorités publiques, opérateurs de services essentiels, fournisseurs de service numérique, infrastructures critiques, etc.).
[17] Art. 550 *bis*, § 5 du Code pénal.
[18] Art. 1382 du Code civil.

De son côté, l'organisation responsable se doit de réagir dans un délai raisonnable en implémentant une solution ou à tout le moins en informant les utilisateurs des systèmes d'information concernés par la vulnérabilité. En effet, l'organisation pourrait, par exemple, voir sa responsabilité engagée pour avoir laissé dans l'ignorance ses clients quant à l'existence de la vulnérabilité (voir ci-après point e).

Il peut s'avérer également particulièrement utile, lorsque les risques principaux de sécurité sont écartés, de publier les informations sur les vulnérabilités découvertes et leur résolution, dans un contexte adéquat[19], afin de faire progresser les recherches en sécurité informatique.

L'intérêt d'une CVDP réside donc dans l'établissement d'un cadre juridique qui renforce la confidentialité et encadre au mieux une éventuelle divulgation publique.

e. Renforcer le respect des obligations légales en matière de sécurité des technologies de l'information

La mise en œuvre d'une politique de divulgation coordonnée permet de prouver les efforts de l'organisation pour le respect de ses obligations légales de sécurité de ses réseaux et systèmes d'information : Règlement général sur la protection des données UE n°2016/679 (« RGPD »), loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (« loi NIS »), règles de responsabilité civile, Code de droit économique, etc.

Tout d'abord, l'article 32 du RGPD prévoit que le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en tenant compte de l'état des connaissances, des coûts de mise en

[19] Par exemple, dans une publication scientifique ou dans un rapport technique diffusé au sein des chercheurs en sécurité informatique.

œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques (dont le degré de probabilité et de gravité varie).

La disposition précise que le responsable du traitement et le sous-traitant peuvent utiliser notamment :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Dans sa recommandation relative aux mesures de sécurité à respecter afin de prévenir les fuites de données (n°01-2013), la Commission de la protection de la vie privée (devenue aujourd'hui l'Autorité de protection des données) rappelle l'importance de documenter, auditer et améliorer aussi souvent que nécessaire les mesures de sécurité de l'information[20].

De la même manière, les lignes directrices pour la sécurité de l'information de données à caractère personnel de l'ancienne Commission de la protection de la vie privée mentionnaient que « le responsable de traitement se doit régulièrement d'organiser un audit de qualité concernant la sécurité de l'information des données à caractère personnel et de prendre des mesures de gestion visant à garantir la confidentialité et l'intégrité des données »[21].

[20] Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données (n°01-2013), www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf, p. 3, point 6.
[21] Commission de la protection de la vie privée, *Lignes directrices pour la sécurité de l'information de données à caractère personnel*, (version 2.0 déc. 2014), pp. 20 et 27, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Richtsnoeren_CBPL_V%202%200%20FR_TRA.pdf.

Or, la mise en œuvre d'une CVDP est une mesure technique et organisationnelle, parmi d'autres mesures, appropriée pour démontrer les efforts du responsable de traitement pour, d'une part, garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes de ses systèmes de traitement[22] et, d'autre part, tester, analyser et évaluer régulièrement l'efficacité des mesures de sécurité du traitement[23]. Les standards techniques internationaux en matière de sécurité des technologies de l'information conseillent d'ailleurs explicitement la mise en œuvre d'une CVDP (voy. par exemple : les normes internationales ISO/IEC 29147[24] et 30111[25]).

L'organisation responsable peut ainsi s'appuyer sur sa CVDP pour démontrer, auprès des autorités de contrôle, ses efforts pour évaluer et gérer les risques liés aux vulnérabilités des systèmes d'information de l'organisation concernée.

Dans le même ordre d'idée, une CVDP peut permettre au responsable de traitement d'être mieux informé sur les éventuelles violations de données à caractère personnel et d'évaluer celles qui doivent, dans les meilleurs délais, faire l'objet d'une notification à une autorité de contrôle[26] ou d'une communication à une personne physique[27].

---

[22] Art. 32 (1), point b du RGPD.
[23] Art. 32 (1), point d du RGPD.
[24] ISO/IEC 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité (https://www.iso.org/standard/72311.html).
[25] ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (https://www.iso.org/standard/53231.html).
[26] Art. 33 du RGPD prévoit que le responsable du traitement doit notifier les violations de données à caractère personnel à l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Le sous-traitant doit également notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.
[27] Art. 34 du RGPD impose que le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

Ensuite, l'article 20 de la loi NIS impose que l'opérateur de services essentiels (« OSE ») prenne « les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information dont sont tributaires ses services essentiels. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances techniques ».

L'OSE doit également prendre « les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services »[28].

Les mesures de sécurité sont définies par la loi NIS comme permettant à un système de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles[29]. Pour adopter les mesures nécessaires et proportionnées aux risques[30], il est nécessaire d'identifier les risques d'incidents et d'en limiter l'impact sur la sécurité des réseaux et des systèmes d'information.

En l'occurrence, la mise en œuvre d'une CVDP offre la possibilité pour un OSE ou un fournisseur de service numérique de mieux connaître les éventuelles vulnérabilités et les menaces susceptibles d'apparaître dans ses réseaux et systèmes d'information afin de répondre de manière adéquate aux exigences de la loi NIS.

---

[28] Art. 20 de la loi NIS ; voy. également l'art. 33 de la loi NIS pour les mesures de sécurité des fournisseurs de service numériques (FSN) – par exemple, les fournisseurs de service d'informatique en nuage (« cloud »).
[29] Art. 6, 9° de la loi NIS.
[30] Art. 6, 15° de la loi NIS définit le risque comme « toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ».

En outre, le Règlement européen sur la Cybersécurité (« Cyber Security Act »)[31] prévoit qu'un schéma européen de certification de cybersécurité doit comprendre au moins les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment[32] dans des produits TIC[33], services TIC[34] et processus TIC [35].

Le Règlement impose ainsi au fabricant ou au fournisseur de produits TIC, services TIC ou processus TIC certifiés de mettre à la disposition du public les informations de contact du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité[36].

Par ailleurs, la responsabilité civile (contractuelle ou extra-contractuelle) d'une organisation responsable peut être engagée lorsqu'une faille de sécurité de ses technologies a causé un dommage à un tiers[37].

Enfin, l'organisation responsable qui vend des systèmes d'information est tenue de garantir ses clients contre les défauts cachés ou les défauts de conformité des biens vendus[38]. Elle peut également être tenue, en qualité de producteur d'un produit (bien corporel) ou d'un service, de la sécurité de ses

[31] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013.
[32] Art. 54, 1, m du Règlement sur la Cybersécurité.
[33] Un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information (art. 2, 12 du Règlement sur la Cybersécurité).
[34] Un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information (art. 2, 13 du Règlement sur la Cybersécurité).
[35] Un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance (art. 2, 14 du Règlement sur la Cybersécurité).
[36] Art. 55, 1, c du Règlement sur la Cybersécurité.
[37] Art. 1382 du Code civil.
[38] Voy. art. 1641 et 1625 du Code civil pour la garantie contre les vices cachés ou art. 1649 *bis* et s. du Code civil sur la garantie contre les défauts de conformité pour les ventes à des consommateurs.

produits et services[39]. La conformité à cette obligation générale de sécurité peut être évaluée en prenant en compte des normes nationales ou internationales, des codes de bonne conduite en vigueur dans le secteur concerné, de l'état actuel des connaissances et de la technique, et la sécurité à laquelle les consommateurs peuvent raisonnablement s'attendre[40].

C. BONNES PRATIQUES

Actuellement, il existe de nombreuses entreprises qui appliquent déjà, en Belgique, des politiques de divulgation coordonnée des vulnérabilités et font appel à des plates-formes de « bug bounty ».

Deux standards internationaux ISO/IEC existent en matière de CVDP : ISO/IEC 29147[41] et ISO/IEC 30111[42]. Le premier décrit la procédure de divulgation d'une vulnérabilité, tandis que le second aborde les processus de traitement de la vulnérabilité renseignée. Ces deux standards décrivent un modèle complet des différents aspects d'une CVDP.

L'ENISA (Agence de l'Union européenne pour la Cybersécurité) a également publié des recommandations sur les bonnes pratiques relatives à la mise en place d'une CVDP[43].

[39] Voy. art. IX.2 et s. du Code de droit économique.
[40] A défaut de normes harmonisées européennes.
[41] ISO/IEC 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité (https://www.iso.org/standard/72311.html).
[42] ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (https://www.iso.org/standard/53231.html).
[43] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure; Art . 6 (1), b du Règlement (UE) 2019/881 charge d'ailleurs l'ENISA d'assister les États membres de l'Union et les institutions européennes, pour établir et mettre en œuvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités.

** Colored-security-background-flat-design Free licence - Designed Freepik - 2020*

I. Contenu d'une CVDP

a. Personnes habilitées

La politique doit être adoptée par les personnes ou les organes pouvant valablement représenter l'organisation responsable et non, par exemple, par un membre de l'équipe informatique sans être valablement mandaté pour ce faire[44]. En effet, les autorisations prévues dans le cadre de la politique

[44] Sous réserve de la théorie du mandat apparent ou du principe général de droit du respect dû aux anticipations légitimes d'autrui.

de divulgation coordonnée doivent nécessairement provenir d'une personne habilitée à cette fin par le titulaire des droits sur le système ou l'équipement concerné[45].

b. Publicité

La publicité donnée à la politique de divulgation responsable est un élément important de son succès[46]. Son contenu doit ainsi être facilement accessible aux participants potentiels, de préférence sur le site internet de l'organisation responsable. Pour ce faire, l'existence de la CVDP devrait être reprise de manière claire et visible sur le site internet de l'organisation responsable (par exemple avec un onglet spécifique ou une sous-section qui contient le contenu complet de la politique)[47]. A ce propos, il existe des propositions de standardisation visant à localiser la CVDP d'une organisation dans un fichier nommé « security.txt » à un endroit connu de l'arborescence de chaque site internet[48] ou des extensions pour navigateur internet qui permettent de renseigner les sites internet qui disposent d'une CVDP[49].

En cas de recours à un programme de récompense pour la découverte de vulnérabilités via une plate-forme de bug bounty, il convient aussi de faire figurer le contenu complet de la CVDP sur cette plate-forme[50].

La CVDP devrait être rédigée dans toutes les langues utilisées par le site internet et dans la mesure du possible aussi en anglais. Il peut s'avérer utile également de mettre un lien à d'autres endroits vers la

[45] Celui-ci est, par défaut, le propriétaire du système.
[46] Pour éviter de commettre une infraction (accès non autorisé à un système d'information), il est nécessaire que la politique de divulgation coordonnée existe préalablement à toute démarche accomplie par le participant. La meilleure façon d'éviter des doutes sur l'existence ou non d'une politique de divulgation coordonnée des vulnérabilités est d'en assurer la publicité. (voir partie II. Aspects légaux). Il est toutefois possible à l'organisation d'avoir une CVDP non publique et limitée à certains participants préalablement sélectionnés (voir notamment certains bug bounty privés).
[47] Par exemple : https://www.[organisation].be/security ou /disclosurepolicy ou encore /vulnerability-policy.
[48] Voy. le projet https://securitytxt.org/
[49] Voir par exemple, l'extension YesWeHack VDP Finder pour Chrome et Firefox.
[50] Par exemple, www.intigriti.be; www.yeswehack.com; www.bugcrowd.com; www.hackerone.com.

page dédiée à la CVDP (par exemple, dans la rubrique aide du programme, dans le mode d'emploi, dans la licence d'utilisation, etc.).

Enfin, il est important pour l'organisation responsable d'informer ses éventuels sous-traitants du contenu de sa CVDP et d'adapter si besoin ses contrats de sous-traitance.

c. Point de contact

L'organisation responsable doit désigner dans sa politique un point de contact vers lequel toutes les informations relatives aux vulnérabilités peuvent être envoyées. A cet effet, une adresse de courriel spécifique pourrait être dédiée à cet effet[51]. Dans le même ordre d'idée, l'organisation responsable doit s'assurer que les courriels reçus par d'autres adresses de courriel [52] soient bien redirigés en interne vers ce point de contact.

L'utilisation d'un formulaire en ligne est aussi intéressant pour recevoir les informations relatives aux vulnérabilités découvertes. Ce procédé offre l'avantage d'automatiser l'encodage, le traitement des données et l'envoi d'un accusé de réception.

De plus, il peut être utile de mentionner les coordonnées de téléphone du service ou de la personne compétente pour traiter les notifications relatives aux vulnérabilités informatiques.

Enfin, il faut préciser clairement les informations à fournir par le participant (voir ci-après, la partie II Procédure).

[51] Comme par exemple : vulnerabilitypolicy@organisation.com; security@organisation.com; csirt@organisation.com; support@organisation.com; security-alert@organisation.com, etc.
[52] Par exemple, info@organisation.com ou contact@organisation.com.

d. Sécurité et confidentialité des communications

Il s'agit d'une question primordiale car il faut éviter au maximum les risques de fuites des informations liées aux vulnérabilités, en garantissant au mieux la confidentialité et l'intégrité des communications.

L'utilisation d'un mode de communication sécurisé est donc hautement recommandé. Celui-ci peut consister à utiliser un moyen pour chiffrer les données[53], créer un portail internet sécurisé[54] ou au moins protéger les documents par un mot de passe[55]. Dans les modalités de communication recommandées aux participants, l'organisation responsable doit donc tenir compte tout spécialement de la sécurité de celles-ci[56].

e. Description des obligations réciproques

1. Champ d'application de la politique

L'organisation responsable doit définir explicitement le champ d'application de sa politique de divulgation coordonnée : quels sont les sites, les produits, les équipements, les services, les systèmes ou les réseaux concernés où sa politique est applicable.

Idéalement, l'organisation responsable devrait veiller à rendre applicables les règles de sa CVDP à ses différents systèmes d'information et à ses engagements contractuels (fournisseurs, clients, sous-traitants, personnel, etc.).

---

[53] Par exemple, Transport Layer Security (TLS) ou son prédécesseur Secure Sockets Layer (SSL) , Secure Multipurpose Internet Mail Extensions (S/MIME), et Pretty Good Privacy (PGP).
[54] en HTTPS ou par un chiffrement dans le navigateur internet.
[55] Le mot de passe étant transmis idéalement à l'organisation responsable par le participant par un autre moyen de communication (téléphone, sms, application de messagerie, autre adresse de courriel, etc.).
[56] Par exemple, fournir la clé publique et le fingerprint de son point de contact pour communiquer de manière chiffrée ou sécuriser en HTTPS son formulaire en ligne.

Dans le cas contraire, la CVDP devrait expressément lister les systèmes d'information appartenant à des tiers et qui seraient exclus du champ d'application de la politique (en l'absence d'autorisation de ces tiers). En cas de doute sur les limites de la CVDP, il convient pour le participant de solliciter préalablement l'accord de l'organisation responsable avant de poursuivre ses recherches.

Egalement, la CVDP devrait mentionner clairement que les recherches du participant sur des systèmes d'information non explicitement inclus dans le cadre de la politique pourraient entraîner des poursuites judiciaires à son encontre (par le ministère public, l'organisation responsable ou des tiers à la CVDP).

2. Conditions de la politique

L'existence même d'une politique de divulgation coordonnée des vulnérabilités, ou d'un programme de bug bounty, implique nécessairement l'octroi au participant d'une autorisation d'accès au système informatique au moins tacite[57]. De même, le participant dispose, en principe, d'une autorisation d'introduire ou de tenter d'introduire des données informatiques dans le système concerné (*voir le Guide – Partie II Aspects légaux*).

L'organisation responsable doit néanmoins mentionner clairement, dans sa politique de divulgation coordonnée, les conditions dans lesquelles les participants peuvent accéder au système informatique, tenter d'introduire ou de modifier des données. Les actions qui sont ou non permises doivent être identifiées, sans ambiguïté sur base des finalités poursuivies.

L'autorisation de modifier ou de supprimer des données informatiques[58] dépend de la manière dont la politique de divulgation coordonnée des vulnérabilités est rédigée. Lors de la rédaction d'une telle politique, l'organisation responsable devra évaluer les avantages, les conditions particulières imposées et les risques encourus afin d'autoriser ou non ces actions. Il devrait être mentionné que le participant doit respecter strictement les conditions de la politique quant à la modification et la suppression de

[57] En fonction du libellé exact de ses dispositions, la politique de divulgation coordonnée des vulnérabilités contiendra des dispositions pouvant être qualifiées d'autorisations soit expresses, soit tacites.
[58] ou de tenter de telles actions.

données informatiques, à défaut de quoi il se rendrait coupable d'une infraction de violation de données informatiques.

A titre d'exemple, il est une bonne pratique d'interdire le recours à des attaques par déni de service distribuée (DDoS) ou par ingénierie sociale, l'installation de logiciels malveillants ou de virus, le vol de mot de passe, le « phishing » par courriel, le spamming, la suppression ou le changement de données/paramètres du système, etc.

La CVDP devrait exclure explicitement les tentatives intentionnelles[59] d'intercepter, d'enregistrer ou de prendre connaissance de communications non accessibles au public ou de communications électroniques[60]. Néanmoins, il pourrait être admis que le contenu d'une communication soit révélé, de manière strictement fortuite, aux participants dans le cadre de la recherche des vulnérabilités[61].

De même, il devrait être mentionné que le participant ne peut utiliser, détenir, révéler ou divulguer des communications non accessibles au public ou des données d'un système informatique dont il ne peut raisonnablement ignorer qu'elles ont été obtenues illégalement.

Il devrait être interdit aussi pour le participant d'installer ou de faire installer un appareil permettant l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public, sauf s'il peut démontrer qu'il agit sans l'intention d'utiliser l'appareil concerné aux fins précitées, soit avec le consentement de tous les participants à la communication, soit en participant lui-même à la communication.

3. Notification

La CVDP doit préciser clairement les informations souhaitées du participant lors de la notification d'une vulnérabilité : type de la vulnérabilité, détails de la configuration, opérations effectuées, outils utilisés,

[59] Ce qui est différent d'une interception fortuite (voir Guide Partie II Aspects légaux).
[60] Sauf l'hypothèse plutôt rare où le participant disposerait du consentement de tous les participants ou participerait lui-même à la communication électronique.
[61] Voy. le secret des communications électroniques (loi du 13 juin 2005).

date des tests, preuves, adresse IP ou URL du système affecté, capture d'écran, coordonnées de contact, etc.

4. Proportionnalité

De manière générale, le participant doit s'engager dans ses actions à respecter le principe de proportionnalité, c'est-à-dire de ne pas perturber la disponibilité des services fournis par le système et de ne pas faire usage de la vulnérabilité au-delà de ce qui est strictement nécessaire à la démonstration de la faille de sécurité. Son attitude doit rester proportionnée : si la démonstration est établie à petit échelle, il n'est pas nécessaire de l'étendre plus loin.

Si cela n'est pas nécessaire à la démonstration de l'existence de la vulnérabilité informatique, l'utilisation des données à caractère personnel par le participant doit être expressément exclue.

En outre, la politique de divulgation coordonnée doit mentionner clairement que les participants ne peuvent détenir plus longtemps que nécessaire les données de l'organisation responsable, dont d'éventuelles données à caractère personnel. Toutes les données personnelles collectées par le participant devraient être supprimées immédiatement. Si cela s'avère nécessaire de conserver ces données encore pendant un certain temps, le participant doit veiller à ce que ces données sont conservées en toute sécurité durant cette période.

5. Confidentialité

L'un des éléments essentiels d'une politique de divulgation coordonnée doit être le respect de la confidentialité : le participant doit s'abstenir de partager ou de divulguer les informations récoltées avec des tiers, sans l'accord explicite de l'organisation responsable[62].

[62] A nouveau, sous réserve d'une diffusion restreinte aux autorités compétentes en matière de Cybersécurité.

De même, toute révélation ou divulgation par le participant de données informatiques, de données de communication ou de données à caractère personnel à des personnes tierces à l'organisation responsable doit être expressément exclue, sauf autorisation préalable de l'organisation responsable.

Le texte de la politique de divulgation coordonnée devrait mentionner que l'objectif de la politique n'est pas de permettre la prise de connaissance intentionnellement du contenu de données informatiques, de données de communication ou de données à caractère personnel et qu'une telle prise de connaissance ne pourrait intervenir que de manière fortuite et incidente dans le cadre de la recherche de vulnérabilités dans les technologies concernées.

6. Exécution de bonne foi

L'organisation responsable du système d'information doit s'engager à exécuter de bonne foi sa politique de divulgation coordonnée et de ne pas poursuivre en justice, au civil ou au pénal, le participant qui en respecte les conditions.

De son côté, le participant doit être dénué d'intention frauduleuse, de dessein de nuire, de volonté de faire usage ou de provoquer un dommage au système visité ou encore à ses données. Cela vaut également pour les systèmes tiers situés en Belgique ou à l'étranger.

S'agissant des dispositifs permettant de commettre une violation de données informatiques, le participant pourrait élaborer, détenir ou mettre à disposition de tels dispositifs dans le cadre de la participation à une politique de divulgation des vulnérabilités. Ces actions ne sont pas illicites tant qu'elles sont justifiées par des fins légitimes de recherches de vulnérabilités avec l'accord de l'organisation du responsable du système informatique concerné.

7. Traitement de données à caractère personnel

L'objet d'une CVDP n'est pas d'effectuer intentionnellement des traitements de données à caractère personnel mais il est possible que le participant doive, même de manière fortuite, traiter des données à caractère personnel dans le cadre de ses recherches de vulnérabilités.

Or, le traitement de données à caractère personnel a une portée large et inclut notamment la conservation, la modification, l'extraction, la consultation, l'utilisation ou la communication de toute information pouvant se rapporter à une personne physique identifiée ou identifiable. Le caractère « identifiable » de la personne ne dépend pas de la simple volonté d'identification de celui qui traite les données mais de la possibilité d'identifier, directement ou indirectement, la personne à l'aide de ces données (par exemple : une adresse de courriel, numéro d'identification, identifiant en ligne, adresse IP ou encore des données de localisation).

Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[63].

Dès lors que la CVDP constitue une forme de contrat d'adhésion qui lie le hacker éthique à l'égard de l'organisation responsable, il s'avère nécessaire d'y préciser les obligations des parties en matière de traitements de données à caractère personnel, notamment les finalités et les moyens essentiels des éventuels traitements effectués dans le cadre de cette politique (*voir Guide – partie II Aspects légaux)*.

8. Délais de procédure

Il est recommandé de fixer des délais clairs à respecter pour chaque étape du processus, notamment pour l'envoi d'un accusé de réception au participant, la communication d'information complémentaire, les investigations, le développement d'une solution, la réponse au participant, l'octroi d'une récompense ou une éventuelle publication. Toutefois, il faut laisser une possibilité de flexibilité des délais, en fonction de la complexité de la vulnérabilité, du nombre de systèmes affectés, de l'urgence ou de la gravité d'une situation.

9. Communication continue

[63] Art. 4, 7) du RGPD.

Une bonne collaboration passe par une communication continue et efficace. Les renseignements fournis par le participant peuvent, en effet, s'avérer très utiles pour identifier la vulnérabilité, y apporter une solution. Il est donc important d'accuser réception de ses envois, de le tenir informé des suites données à sa notification, de lui rappeler le contenu de ses obligations et de lui préciser les prochaines étapes de la procédure.

Par ailleurs, l'intervention d'un coordinateur (désigné de préférence dans la CVDP) ou d'une plate-forme proposant des récompenses pour la découverte de vulnérabilités peut faciliter l'établissement et le maintien d'une relation constructive entre les parties ou éventuellement garantir l'anonymat du participant.

En l'absence de réaction de l'une des parties ou du coordinateur désigné, les parties peuvent toujours faire appel au Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be).

10. Octroi d'une récompense

L'octroi d'une récompense ou d'une reconnaissance publique[64] par l'organisation responsable augmente l'attractivité de la CVDP pour les participants et offre souvent de meilleurs résultats pour les organisations. Il peut même s'agir d'un simple cadeau symbolique : par exemple, un t-shirt, un autocollant ou une tasse spécifique.

Dans le cadre d'un programme de récompense pour la découverte de vulnérabilités (ou bug bounty), la récompense est fixée en fonction du nombre, de l'importance ou de la qualité des informations transmises.

[64] classement parmi les meilleurs participants, publication, conférence, etc.

Il est essentiel que la nature de cette récompense soit préalablement et clairement fixée par l'organisation responsable dans sa politique. Toute demande de récompense en dehors des conditions définies par la CVDP pourra ainsi être assimilée à une tentative illicite d'extorsion.

L'organisation peut utilement avoir recours à une plate-forme de *bug bounty*[65] qui coordonnera avec elle les aspects techniques et administratifs de son programme de récompense.

11. Eventuelle divulgation publique

L'éventuelle divulgation de la vulnérabilité doit se réaliser de manière coordonnée et synchronisée entre les parties, afin de fournir un temps suffisant à l'organisation responsable pour résoudre le problème et informer préalablement les opérateurs critiques affectés.

Lorsqu'une vulnérabilité est identifiée dans un programme, un composant, un protocole ou un format fourni par un fournisseur tiers, l'organisation responsable doit l'en informer directement et ce avant toute divulgation publique.

Il en va de même lorsque la vulnérabilité identifiée risque d'affecter de manière plus large d'autres organisations utilisant une technologie similaire ou lorsque le composant informatique affecté est fourni par l'organisation responsable à d'autres organisations (par exemple, via des licences d'utilisation). Dans ces cas, il est alors indispensable qu'un rapport sur la vulnérabilité et sa solution soit diffusé aux parties concernées afin de leur donner l'occasion de se protéger.

En cas de divulgation publique, le rapport relatif à la vulnérabilité et la solution devraient être diffusés, idéalement, en même temps.

L'organisation responsable devrait proposer différents moyens d'informer et de protéger ses utilisateurs : par exemple la mise à jour automatique du système, la publication d'avis de sécurité sur

[65] Par exemple : www.intigriti.com (plate-forme basée en Belgique); www.yeswehack.com (plate-forme basée en France); www.yogosha.com; www.hackerone.com (plate-forme basée aux USA).

son site internet, la diffusion par courriel avec un lien vers une page internet dédiée, communication de ces informations à son réseau de vendeurs, etc.

Dans l'hypothèse d'une vulnérabilité qui concernerait également d'autres organisations, l'organisation responsable se doit d'en informer, en tout état de cause, le Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be), même si elle ne souhaite pas que la vulnérabilité soit divulguée publiquement.

** tech-support-concept. Free licence. Designed by macrovector / Freepik (2020)*

CENTRE FOR CYBER SECURITY BELGIUM

II. Procédure

a. Découverte

Lorsqu'un participant découvre des informations relatives à une vulnérabilité potentielle, celui-ci devrait, dans la mesure du possible, réaliser au préalable des vérifications permettant de confirmer l'existence de la vulnérabilité et d'identifier les éventuels risques encourus.

Ensuite, il devrait transmettre à l'organisation responsable, au minimum, les informations techniques suffisantes pour permettre la confirmation de cette faille et fournir ses coordonnées de contact. Ces éléments pourraient être complétés en fonction des spécifications de la politique de divulgation coordonnée ou du contenu du formulaire en ligne de l'organisation responsable.

b. Notification

Le participant devrait notifier, dans les plus brefs délais, les informations techniques au point de contact ou au coordinateur désigné par l'organisation responsable, en utilisant des moyens de communication sécurisés.

Lorsqu'elle reçoit une notification, l'organisation responsable devrait envoyer au participant, dans les plus brefs délais, un accusé de réception avec la référence interne de celle-ci et la prochaine étape de la procédure.

Cet accusé de réception serait l'occasion pour l'organisation responsable de rappeler le contenu de sa politique de divulgation coordonnée, ou à tout le moins de transmettre un lien vers celle-ci, et de demander d'éventuelles informations complémentaires.

Il est notamment intéressant de demander si le participant aurait déjà signalé ce problème à d'autres organisations responsables.

c. Investigation

La phase d'investigation permet à l'organisation responsable de reproduire l'environnement et le comportement signalé afin de vérifier les informations communiquées.

Il convient de tenir informé de manière régulière le participant des résultats des investigations et des suites données à la notification.

Durant ce processus, les parties doivent veiller à faire le lien avec des rapports de sécurité similaires ou connexes, à évaluer le risque et la gravité de la vulnérabilité, et à déterminer les éventuels autres produits ou systèmes affectés.

d. Déploiement d'une solution

L'objectif de la politique de divulgation est de permettre le développement et de déploiement d'une solution afin de faire disparaître la vulnérabilité du système informatique.

Sauf si celle-ci est légalement ou contractuellement tenue de le faire, l'organisation responsable demeure libre du choix de développer une solution et de la mettre en œuvre.

Bien entendu, le choix de ne pas résoudre une faille de sécurité avérée pourrait, le cas échéant, engager la responsabilité civile de l'organisation responsable si un dommage devait en résulter pour un tiers[66].

Dans la mesure du possible, la solution devrait être mise au point au plus tard dans les 90 jours calendrier.

Ces délais devraient être raccourcis au strict minimum en cas de mise en danger des utilisateurs des systèmes impactés ou de risques pour la protection des données à caractère personnel. Si

[66] Indépendamment même de l'existence ou non d'une politique de divulgation responsable.

l'organisation est incapable de résoudre le problème immédiatement, le système informatique en question devrait alors être mis hors service complètement à titre temporaire.

Cependant, la chaîne d'approvisionnement (*supply chain*) et la multiplicité des interdépendances entre les systèmes d'information peuvent compliquer le délai nécessaire à l'élaboration d'une solution et son déploiement.

Durant cette phase, l'organisation responsable (ou son prestataire) doit mener, d'une part, des tests positifs pour vérifier que la solution fonctionne correctement et, d'autre part, des tests négatifs pour s'assurer que la solution ne perturbe pas le bon fonctionnement des autres fonctionnalités existantes.

Lorsque la solution est prête et que la vulnérabilité concerne également d'autres organisations, celle-ci doit être transmise prioritairement et avant toute divulgation publique au CCB (vulnerabilityreport@cert.be).

L'organisation responsable devrait respecter un délai raisonnable à partir de cette transmission avant une éventuelle divulgation générale aux utilisateurs, afin de permettre aux opérateurs d'intérêt vital (opérateurs de services essentiels NIS, infrastructures critiques, administrations publiques, etc.) d'implémenter prioritairement la solution.

e. Eventuelle divulgation publique

Sauf obligation légale particulière, la divulgation publique d'une vulnérabilité n'est pas une étape obligatoire d'une CVDP. En effet, le participant et l'organisation responsable peuvent convenir de ne pas divulguer publiquement l'existence de la vulnérabilité. Cela pourrait être le cas si celle-ci s'avère trop difficile ou impossible à résoudre, ou si sa résolution impliquera des coûts démesurés en comparaison avec les éventuels risques encourus.

Cela doit toutefois rester l'exception dans la mesure où l'objectif d'une CVDP est d'améliorer la sécurité et la transparence vis-à-vis des utilisateurs. Certaines obligations légales imposent, par

ailleurs, l'organisation responsable informe les utilisateurs des systèmes d'information[67] ou les personnes physiques concernées par une violation de données à caractère personnel[68].

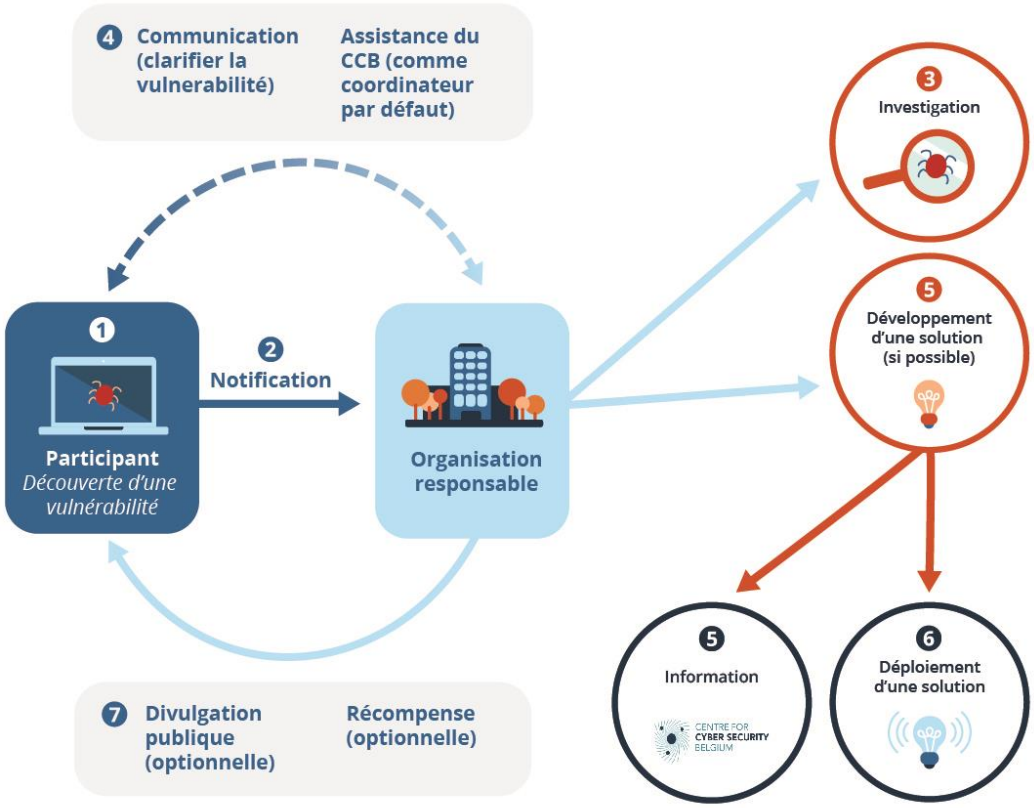
En tout état de cause, les informations relatives à une vulnérabilité qui concernerait également d'autres organisations devraient être divulguées au moins au CCB (vulnerabilityreport@cert.be).

Si la vulnérabilité est rendue publique, l'organisation responsable fixe, en coordination avec le participant, les modalités de sa publication. Idéalement, les informations sur la vulnérabilité et sa solution devraient être diffusés simultanément. Il est recommandé à l'organisation responsable d'informer ses clients par la publication d'un avis de sécurité via son site internet ou d'autres moyens de communication (courriel, lettre d'information, mise à jour du système, etc.).

L'organisation responsable devrait également informer les autres organisations probablement aussi concernées par la même vulnérabilité. L'éventuelle interdépendance des systèmes d'information ou la chaîne d'approvisionnement peut impliquer une coordination plus large de l'éventuelle divulgation.

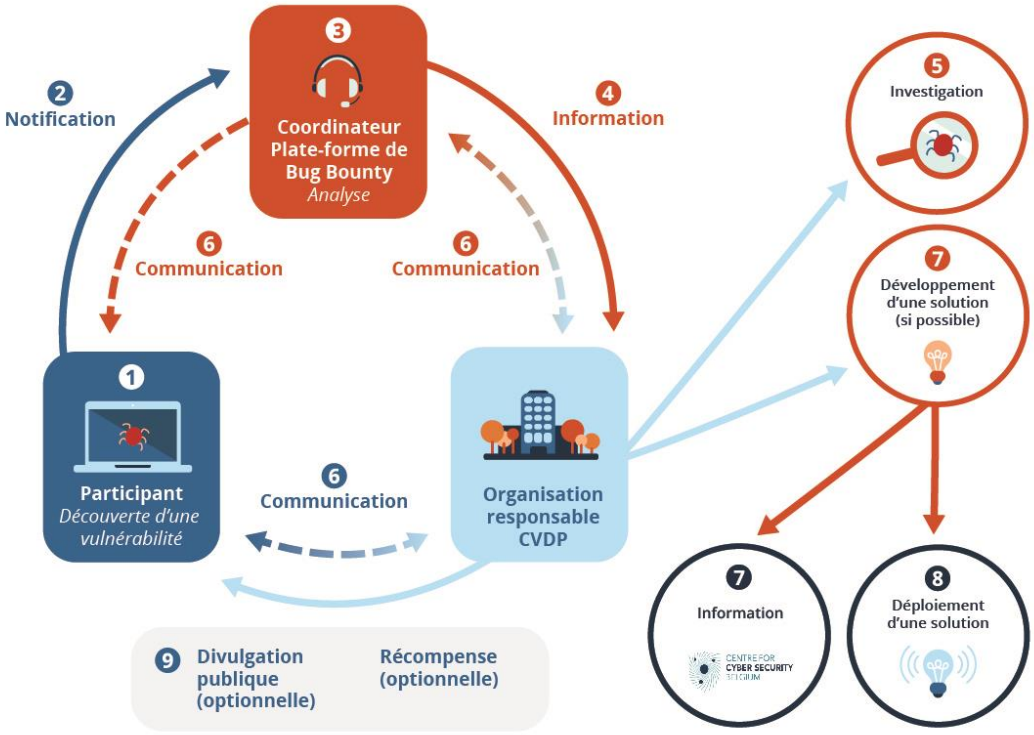
Il convient aussi de recueillir les commentaires des utilisateurs sur le déploiement de la solution et de prendre les mesures correctives nécessaires pour régler les éventuels problèmes posés par la solution, notamment de compatibilité avec d'autres produits ou services.

[67] Voir les règles de responsabilité contractuelle et extra-contractuelle notamment.
[68] Art. 34 du RGPD.



1. Le participant trouve une vulnérabilité dans le cadre d'un CVDP.
2. Le participant informe l'organisation responsable sur la base des détails de la CVDP.
3. L'organisation responsable analyse la vulnérabilité.
4. Communication continue entre le participant et l'organisation responsable afin de clarifier la vulnérabilité. L'assistance du CCB (en tant que coordinateur par défaut) peut être demandée s'il y a un manque de communication lors de ce processus.
5. Une solution est élaborée (si possible). Dans le cas où la vulnérabilité peut également affecter d'autres organisations, l'organisation responsable en informe le CCB.
6. L'organisation responsable déploie la solution auprès de ses utilisateurs ou clients.
7. La divulgation publique peut être discutée et une récompense peut être accordée sur la base de la CVDP.

** Designed by CCB and Intigriti - 2020*



1. Le participant trouve une vulnérabilité dans le cadre d'un CVDP.
2. Le participant informe l'organisation responsable par l'intermédiaire d'un coordinateur, par exemple une plateforme de bug bounty, sur la base des détails de la CVDP.
3. Le coordinateur analyse la vulnérabilité.
4. Après validation, le coordinateur informe l'organisation responsable.
5. L'organisation responsable analyse la vulnérabilité.
6. 6 Communication continue entre le participant et l'organisation responsable afin de clarifier la vulnérabilité, si souhaité à travers le coordinateur.
7. 7 Une solution est élaborée (si possible). Dans le cas où la vulnérabilité peut également affecter d'autres organisations, l'organisation responsable en informe le CCB.
8. L'organisation responsable déploie la solution auprès de ses utilisateurs ou clients.
9. La divulgation publique peut être discutée et une récompense peut être accordée sur la base de la CVDP.

** Designed by CCB and Intigriti - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

D. REFERENCES

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure et *Economics of Vulnerability Disclosure*, 2018, www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

CENTRE FOR EUROPEAN POLICY STUDIES (CEPS), *Software vulnerability disclosure in Europe. Technology, Policies and Legal Challenges, Report of a CEPS Task Force, 2018,* www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges

GLOBAL CONFERENCE CYBER SPACE, *Best practice guide Responsible Disclosure*, 2015, www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf

INTERNET ENGINEERING TASK FORCE (IETF) - CHRISTEY S. & WYSOPAL C., *Responsible Vulnerability Disclosure Process*, 2002, https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00 (www.circl.lu/pub/responsible-vulnerability-disclosure)

ORGANIZATION FOR INTERNET SAFETY, *Guidelines for responsible disclosure*, 2004, www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf

SOFTWARE ENGINEERING INSTITUTE, *The CERT Guide to Coordinated Vulnerability Disclosure, 2013 (updated in 2019)* https://vuls.cert.org/confluence/display/CVD

NATIONAL CYBER SECURITY CENTRE (NL), *Leidraad Coordinated Vulnerability Disclosure (Coordinated Vulnerability Disclosure: the Guideline),* 2019, //english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline et *Policy for arriving at a practice for Responsible Disclosure*, 2013

CIO PLATFORM NEDERLAND - CEG INFORMATION SECURITY, *Coordinated Vulnerability Disclosure. Model Policy and Procedure*, 2016, www.cio-platform.nl/en/publications et *Coordinated Vulnerability Disclosure 1.4. Implementation guide*, 2016, www.cio-platform.nl/en/publications

ISO/IEC 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité (https://www.iso.org/standard/72311.html)

ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (https://www.iso.org/standard/53231.html)

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE SUR LES POLITIQUES DE DIVULGATION COORDONNEE DES VULNERABILITES
PARTIE I : LES BONNES PRATIQUES

Ce document et ses annexes ont été élaborés par le Centre pour la Cybersécurité Belgique (CCB), administration fédérale créé par l'arrêté royal du 10 octobre 2014 et sous l'autorité du Premier Ministre.

Le CCB décline toute responsabilité éventuelle en lien avec le contenu de ce document.

Les informations fournies :
• sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
• ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éd. Responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépôt légal :
D/2020/14828/012

2020