CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

LES POLITIQUES DE DIVULGATION COORDONNÉE DES VULNÉRABILITÉS

COORDINATED VULNERABILITY DISCLOSURE POLICIES

Les politiques de divulgation coordonnée des vulnérabilités *(Coordinated Vulnerability Disclosure Policies – "CVDP")*

Chaque système informatique ou réseau peut comporter des vulnérabilités. Ces vulnérabilités peuvent être détectées tant par des personnes bien intentionnées que par des personnes mal intentionnées. Cependant, la peur d'être poursuivi en justice empêche souvent les personnes bien intentionnées ("*hackers éthiques*") de signaler les vulnérabilités.

L'accès ou la tentative d'accès sans autorisation dans un système informatique est punissable, même si le système informatique n'est pas sécurisé et que la personne agit avec de bonnes intentions. Lorsque la personne dispose d'une autorisation d'accès au système informatique, les règles juridiques sont néanmoins différentes.

Lorsqu'une organisation applique une politique de divulgation coordonnée de vulnérabilités ou un programme de récompense pour la découverte de vulnérabilités, elle octroie une autorisation d'accès au moins partielle au système informatique concerné.

En effet, l'organisation peut faire appel soit à une entreprise pour vérifier la sécurité de ses systèmes d'information (via un audit de sécurité par exemple), soit à des "hackers éthiques" (via une CVDP ou un bug bounty).

Une politique de divulgation coordonnée de vulnérabilités[1] ***(Coordinated Vulnerability Disclosure Policies – "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 vul-*

[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").*

nérabilités dans ses systèmes, ou à lui transmettre toute information pertinente à ce sujet. Ces 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.

Un programme de récompense pour la découverte de vulnérabilités *("bug bounty")*[3] *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 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)*[4].

Actuellement, de nombreuses organisations disposent déjà de CVDP accompagnée ou non d'un "bug bounty".

Afin d'aider les organisations qui souhaitent mettre en œuvre une CVDP, le Centre pour la Cybersécurité Belgique (CCB) a élaboré la présente brochure, un Guide (en deux parties)[5] et propose un modèle de CVDP. Ces documents sont disponibles sur le site du CCB.

D'ailleurs, le CCB a lui-même adopté et publié sa CVDP sur son site internet (*www.ccb.belgium.be/fr/vulnerability-policy*).

---

[3] *En anglais, "vulnerability rewards program" ou "bug bounty program".*

[4] *Voy. par exemple: www.intigriti.com (Belgique); www.yeswehack.com, www.yogosha.com (France); www.zerocopter.com (Pays-Bas); www.hackerone.com, www.bugcrowd.com (USA).*

[5] *Guide sur les politiques de divulgation coordonnée des vulnérabilités, Partie I: Bonnes pratiques et Partie II: Aspects légaux, Centre pour la Cybersécurité Belgique (CCB), 2020 (www.ccb.belgium.be).*

La présente brochure vise à exposer (en résumé) les concepts, les objectifs, les questions juridiques et les bonnes pratiques liées à l'adoption d'une CVDP dans l'état actuel de la législation en Belgique – voir pour de plus amples détails le Guide CVDP (Partie I et II), ainsi que l'exemple de CVDP.

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.

Pour les organisations:

Quels sont les avantages pour votre organisation d'adopter une CVDP?
La mise en œuvre d'une CVDP:

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

La politique de divulgation coordonnée de vulnérabilités constitue une forme de contrat d'adhésion dans lequel toutes les dispositions contractuelles sont fixées par l'organisation responsable 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 Partie II: Aspects légaux*).

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). 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.

b) augmente la sécurité des systèmes d'information et encourage les recherches.

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. 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.

c) assure 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) garantit la confidentialité.

La divulgation complète d'une vulnérabilité, alors que celle-ci existe toujours auprès de nombreux utilisateurs, constitue un risque important de sécurité en matière de technologies de l'information. En effet, des tiers malveillants pourraient développer et répandre des outils spécifiques pour exploiter cette vulnérabilité. 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. 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) renforce 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. (*voir Guide Partie I: Bonnes pratiques*).

Chaque organisation peut en fixer les règles précises à condition de reprendre certains éléments, de façon à ce que la politique puisse pleinement sortir ses effets juridiques. Ainsi, nous recommandons de prendre les mesures suivantes:

- **Personnes habilitées:** faites approuver la politique par une personne habilitée à représenter légalement votre organisation (par exemple, le directeur).
- **Publicité:** le contenu de votre CVDP doit pouvoir être disponible et accessible par le participant: soit sur votre site internet, soit sur le site internet d'un coordinateur (par exemple une plateforme de "bug bounty"). Si possible, celle-ci devrait être rédigée dans les différentes langues de votre site internet. Nous préconisons d'élaborer un texte concis et clair mais complet.
- **Point de contact:** identifiez clairement un point de contact ou utilisez un formulaire en ligne. Communiquez ensuite le plus souvent et le plus efficacement possible avec les participants. Ils pourraient vous aider à savoir si votre solution technique fonctionne.
- **Coordinateur:** il peut s'avérer très efficace de désigner un coordinateur. Par exemple, l'utilisation d'une plateforme de programmes de récompense pour la découverte de vulnérabilités (*"bug bounty platform"*) peut vous permettre de recevoir un nombre plus important de vulnérabilités. Si les participants à la politique ou le coordinateur désigné ne réagissent pas, vous pourrez faire appel, par défaut, au CCB (*vulnerabilityreport@cert.be*) comme coordinateur.
- **Sécurité et confidentialité des communications:** veillez à la sécurité et la confidentialité de vos communications.
- **Champ d'application:** mentionnez clairement à quels sites, produits, appareils, services, systèmes et réseaux s'applique votre CVDP? Choisissez attentivement le champ d'application

de votre politique, sur la base des éléments de votre système que vous êtes en mesure techniquement de surveiller. Excluez tous les systèmes dépendants de tiers qui n'auraient pas donné explicitement leur accord sur les règles de votre CVDP. Si vous n'êtes pas capable de vérifier si la CVDP a été respectée pour certaines composantes de votre système, évitez de les inclure dans le champ d'application de votre CVDP. Ce qui n'est pas mentionné explicitement dans le champ d'application ne relève, en principe, pas du champ d'application de la politique.

- **Conditions:** indiquez clairement ce que peut faire ou non le participant en vue de prouver l'existence d'une vulnérabilité présumée. Les éventuelles modifications de données dans le système informatique doivent être minimes (par exemple, la présence de "visit logs"). Interdisez explicitement l'installation de malware ou de virus, le vol de mots de passe, la suppression ou la modification de paramètres du système, le recours à des attaques de déni de service ("DDOS"), des attaques d'ingénierie sociale ("social engineering"), le hameçonnage ("phishing"), l'envoi massif de courriels non souhaités («spamming»), etc. Excluez l'utilisation, la détention, la révélation ou la divulgation du contenu de communications non accessibles au public ou de données d'un système informatique, dont le participant ne peut raisonnablement ignorer qu'elles ont été obtenues illégalement (comme des mots de passe volés et publiés sur internet).
- **Notification:** précisez clairement les informations souhaitées du participant (type de la vulnérabilité, détails de la configuration, opérations effectuées, outils utilisés, date des tests, preuves, adresse IP ou URL du système affecté, capture d'écran, coordonnées de contact, etc.). Fixez à l'avance les délais de réponse pour l'envoi d'informations sur une vulnérabilité et les autres phases de la procédure. Communiquez ces délais également lors de chaque contact. Conservez le droit à la flexibilité en fonction de la complexité, de l'urgence et de l'ampleur de la vulnérabilité.
- **Proportionnalité:** Imposez aux participants de ne pas dépasser les limites du raisonnable pour prouver une vulnérabilité. Cela sous-entend également que la disponibilité des services de l'organisation responsable ne peut pas être perturbée par les recherches.
- **Confidentialité:** imposez la confidentialité des informations échangées dans le cadre de la politique.

- **Exécution de bonne foi:** engagez-vous à respecter le contenu de votre politique et de ne pas poursuivre en justice, au civil ou au pénal, le participant qui en respecte les conditions.
- **Traitement de données à caractère personnel:** précisez bien les obligations des parties en matière de traitements de données à caractère personnel.
- **Développez et déployez une solution** si possible et dans un délai raisonnable. Informez-en également les participants.
- **Remerciez les participants**, même s'ils mettent le doigt sur des vulnérabilités. Après tout, ils ont tenté d'améliorer la sécurité de votre service. Pour ce faire, adoptez de préférence un programme de récompense pour la découverte de vulnérabilités (*bug bounty program*), en fonction de l'importance de la vulnérabilité. Cette forme de politique est plus attrayante pour les éventuels participants et souvent plus efficace pour votre organisation. La récompense peut prendre différentes formes: financière, cadeau ou simple classement public des participants (*Leaderboard*).
- **Donnez la possibilité aux participants de publie**r à propos de la vulnérabilité. Il s'agit souvent pour eux d'une bonne raison de poursuivre leurs recherches. Les publications consacrées à la vulnérabilité (par exemple, sans mention de votre organisation) contribueront à améliorer la sécurité des systèmes d'information.
- **Informez le CCB** (*vulnerabilityreport@cert.be*) et les tiers (ou leurs organisations représentatives) qui pourraient vraisemblablement être aussi impactés par la vulnérabilité.

Pour les participants

Une CVDP offre la possibilité de détecter et de signaler des vulnérabilités de manière légale. Cette opportunité est fondée sur une autorisation, moyennant certaines conditions, et repose sur la confiance réciproque.

Il importe donc que vous lisiez attentivement le contenu de la CVDP avant d'entreprendre la moindre démarche:

- **Respecter les conditions de la CVDP:** veillez à respecter le champ d'application et les conditions de la CVDP.

- **Proportionnalité:** ne dépassez pas les limites du raisonnable pour prouver la vulnérabilité. C'est le fil rouge de toutes vos actions.
  - Si la vulnérabilité peut être démontrée à petite échelle, inutile d'aller plus loin.
  - Réunissez uniquement les preuves nécessaires (téléchargements ou captures d'écran) et de préférence sans données à caractère personnel.
  - Ne perturbez pas la disponibilité du système et n'utilisez la vulnérabilité que pour ce qui est nécessaire pour la démontrer et la documenter.
- **Confidentialité et sécurité des résultats de vos recherches:** ne partagez et ne diffusez avec des tiers aucune information liée aux vulnérabilités découvertes, sauf avec l'autorisation expresse de l'organisation concernée. Veillez aussi à respecter les modes de communication sécurisé recommandés.
- **Soyez le plus exhaustif possible** dans votre rapport. Utilisez également des *timestamps* pour démontrer que vous avez réagi dès que possible après la découverte de la vulnérabilité: vous éviterez ainsi tout doute quant à vos intentions. Efforcez-vous d'effectuer des contrôles en amont afin de confirmer l'existence de la vulnérabilité et d'identifier les risques éventuels.
- **Communication continue:** soyez patient et bienveillant dans votre communication. Il est possible que l'organisation ne sache pas précisément comment réagir adéquatement face à cette vulnérabilité. Il se peut aussi qu'une vulnérabilité ait déjà été signalée à plusieurs reprises sans toutefois sembler constituer un risque.
- **Exécution de bonne foi:** vos actions doivent démontrer que vous êtes 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.
- **Eventuelle divulgation publique:** demandez toujours l'autorisation de l'organisation responsable avant toute divulgation publique sur la vulnérabilité. Attendez également un délai raisonnable (en coordination avec l'organisation) afin qu'une solution puisse être développée et déployée. Une organisation peut toujours choisir de ne pas développer et déployer une solution, sauf si elle y est contrainte par la loi ou par un contrat. Si vous estimez malgré tout qu'une solution devrait être développée, n'entreprenez aucune démarche susceptible de violer la CVDP

et contactez le CCB (*vulnerabilityreport@cert.be*) en tant que coordinateur.

- **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 traiter de telles données dans le cadre de ses recherches de vulnérabilités. Dans ce cas, veillez à respecter vos obligations en matière de protection des données à caractère personnel.
- **Ne demandez pas de récompense**, si cela n'a pas été préalablement et clairement fixé par l'organisation responsable dans sa CVDP/bug bounty. Toute demande de récompense en dehors des conditions définies par la CVDP pourra ainsi être assimilée à une tentative illicite d'extorsion.

Si, par hasard, vous découvrez une vulnérabilité auprès d'une organisation qui n'a pas élaboré de CVDP, n'allez pas plus loin. Si la vulnérabilité est critique, prenez contact avec un coordinateur tiers comme une plate-forme de bug bounty ou à défaut avec le CCB (*vulnerabilityreport@cert.be*). Toute intrusion volontaire et non autorisée dans un système informatique reste punissable en l'absence de CVDP.

Références

Guide sur les politiques de divulgation coordonnée des vulnérabilités: partie I (Bonnes pratiques), Centre pour la Cybersécurité Belgique (CCB), 2020 (*www.ccb.belgium.be*).

Guide sur les politiques de divulgation coordonnée des vulnérabilités: partie II (Aspects légaux), Centre pour la Cybersécurité Belgique (CCB), 2020 (*www.ccb.belgium.be*).

European Union Agency for Network and Information security (ENISA), *Good Pratice 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*

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

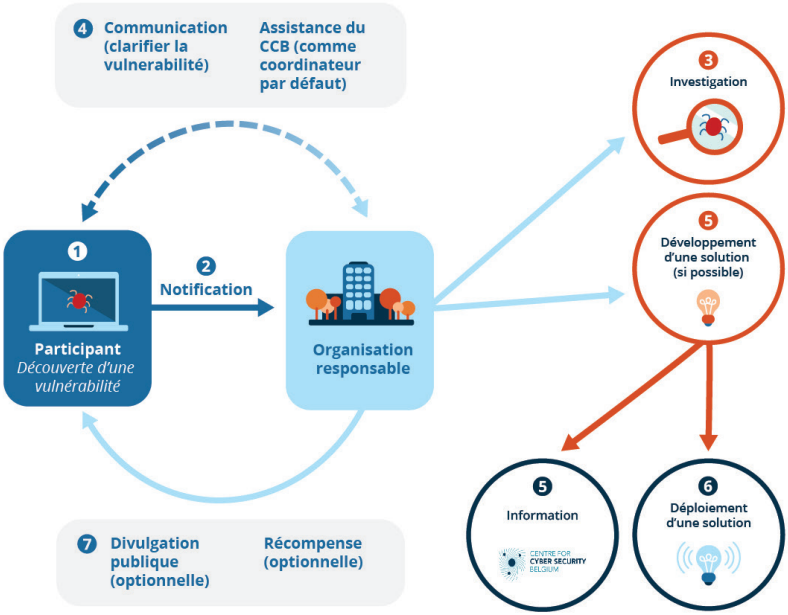
National Cyber Security Centre (NL), *Leidraad Coordinated Vulnerability Disclosure (Coordinated Vulnerability Disclosure: the Guideline)*, 2019, // english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline et *Policy for arriving at a practice for Responsible 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*)

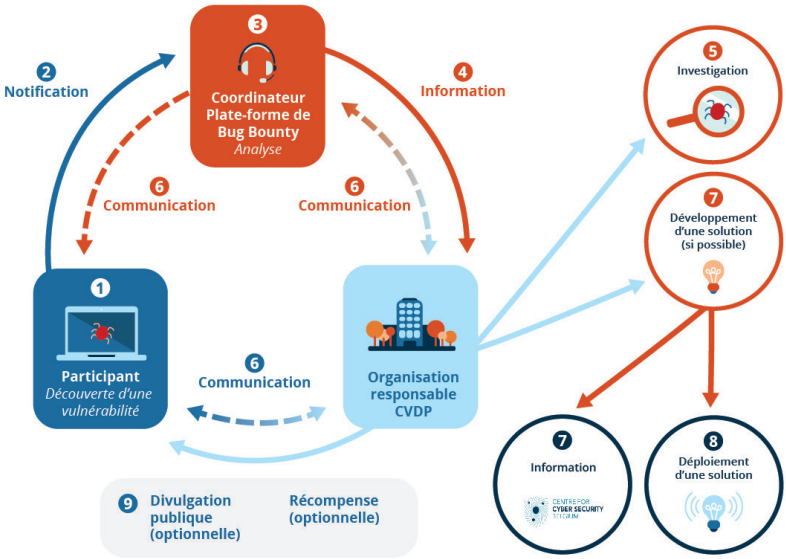
ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (*https://www.iso.org/standard/53231.html*)

CVDP sans coordinateur



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. 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.

CVDP avec coordinateur



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.

Prépresse et impression
Imprimerie centrale de la Chambre des représentants

Bruxelles, octobre 2020

Editeur responsable
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur, Rue de la Loi 16, 1000 Bruxelles

D/2020/14828/010