ébauche

MO – Ch.

Politique créée : 02/12/2021

Pour toute information concernant cette politique, veuillez communiquer auprès du bureau des services d'enquêtes techniques, équipe d'accès et d'interception secrète, à l'adresse RCMP.CAITHQ-EAISQG.GRC@rcmp-grc.gc.ca.

1. Définitions

1.1. **Dispositif informatique** signifie un téléphone cellulaire, un ordinateur, un serveur, une tablette ou tout autre dispositif électronique tel que des caméras sans fil et des serrures intelligentes, qui peuvent être utilisés pour envoyer ou recevoir des données, y compris des communications privées, sur un réseau tel que l'internet.

1.2. **L'équipe d'accès secret et d'interception** (EASI) est chargée de fournir des services électroniques secrets à la GRC et à ses partenaires chargés de l'application de la loi, tel qu'indiqué dans l'art. 5. Cette équipe spécialisée déploie secrètement des outils d'enquête embarqués (OEE) - par un accès à distance, proche ou rapproché - et d'autres outils technologiques permettant l'interception de communications privées et de données de transmission, la collecte d'informations de suivi et de données au repos à partir de dispositifs informatiques. Seuls les opérateurs de l'EASI ont le droit d'utiliser les OEE au sein de la GRC.

1.3. **L'EASI** à la Direction générale nationale (DGN) est le centre des politiques et des opérations situé au sein des Opérations techniques de la GRC à la DGN. Les opérateurs de l'EASI se trouvent à l'administration centrale de l'EASI et dans certaines divisions.

1.4. **L'outil d'enquête embarqués (OEE)** signifie un logiciel développé par la GRC et/ou par l'acquisition de biens sensibles ou non sensibles. Les OEE peuvent être déployés sur des dispositifs ou des réseaux informatiques par un accès à distance, proche ou rapproché. Les OEE permettent d'intercepter des communications privées et des données de transmission, et de recueillir des informations de suivi et des données à l'arrêt à partir de dispositifs et de réseaux informatiques. Un seul OEE peut être programmé avec plusieurs fonctions.

ébauche

1.5 **Les OEE sensibles** sont des OEE qui, si compromis, pourraient nuire gravement aux relations de la GRC avec ses partenaires, ainsi qu'à la capacité de la GRC d'enquêter sur des affaires graves.

1.6 **Les OEE non sensibles** sont des OEE qui, si compromis, pourraient entraver la capacité de la GRC à enquêter sur certaines affaires, mais ne mettraient pas en péril le programme ou les relations avec les partenaires.

1.7. **Le Programme de gestion de cas techniques (PGCT)** représente un groupe consultatif au sein de la Sous-direction des services d'enquêtes techniques (SET) des Opérations techniques qui veille à ce que toutes capacités sensibles soient déployées efficacement de manière légale et conforme à la Charte.

1.8. **Solution technique** signifie un outil ou une technologie, tel qu'un OEE, un logiciel moins sensible qu'un OEE ou une méthode d'accès à un dispositif informatique, qui est soit acquis ou soit développé à l'interne.

2. Généralités

2.1. Toute activités provenant de l'EASI, telles que décrites dans la sec. 5, ne seront menées que par des opérateurs de l'EASI certifiés ou sous la directive d'un opérateur de l'EASI certifié, en consultation avec le QG de l'EASI, et avec toutes les approbations requises.

2.2. Toutes activités de l'EASI seront menées conformément aux autorisations légales, en cas d'urgence ou sur la base d'avis juridiques de la Couronne, obtenus par la Direction des services d'enquête technique (DSET).

3. Rôles et responsabilités

3.1. SIÈGE DE l'EASI

3.1.1. Élaborer et maintenir la politique et les procédures d'exploitation normalisées relatives aux solutions techniques de l'EASI.

3.1.2. Être la seule entité à utiliser, à maintenir et à déployer les OEE et autres actifs sensibles.

3.1.3. Examiner et approuver toutes solutions techniques et autres outils utilisés par les unités divisionnaires de l'EASI afin de garantir une cohérence nationale.

3.1.4. En collaboration avec d'autres unités de la DSET, superviser l'acquisition, la recherche et le développement de solutions techniques et de nouvelles technologies à l'appui de toutes unités de l'EASI.

3.1.5. Développer et maintenir le programme de doublure des opérateurs de l'EASI.
Pour obtenir des informations sur le programme de doublure des opérateurs de l'EASI, veuillez contacter le QG de l'EASI à l'adresse RCMP.CAITHQ-EAISQG.GRC@rcmp-grc.gc.ca.

3.1.6. S'assurer que les statistiques sur l'utilisation des solutions techniques soient compilées selon les directives de la DSET.

3.2. Être commandant divisionnaire de EASI

ébauche

3.2.1. S'assurer que les opérateurs de l'EASI n'utilisent les solutions techniques qu'après avoir consulté le QG de l'EASI, et ce, pour chaque enquête.

3.2.2. S'assurer que l'utilisation et le déploiement des solutions techniques soient conformes aux règles associées à leur classification de sécurité désignée.

3.2.3. Assurer le suivi de l'utilisation des solutions techniques de l'EASI et remettre un compte rendu au siège de l'EASI.

3.2.4. S'assurer que les opérateurs de l'EASI divisionnaires participent au programme de doublure des opérateurs de l'EASI.

3.2.5. S'assurer que toutes les solutions techniques de l'EASI soient déployées conformément à la politique, aux directives et aux conditions de l'autorisation judiciaire pertinentes.

3.3. Être opérateur de l'EASI

3.3.1. Apporter un soutien aux enquêtes criminelles par le déploiement d'OEE et/ou d'autres solutions techniques secrètes sur des réseaux et des dispositifs informatiques, soit à distance, soit par un accès de près ou de loin, afin de recueillir des preuves.

3.3.2. Fournir une assistance technique aux enquêtes sur la cybercriminalité visant à identifier les auteurs et à déterminer l'origine de la cybercriminalité.

3.2.3. Suivre l'utilisation des solutions techniques de l'EASI et rendre un compte rendu au siège de l'EASI.

3.2.4. S'assurer que les opérateurs de l'EASI divisionnaires participent au programme de doublure des opérateurs l'EASI.

3.2.5. S'assurer que toutes les solutions techniques de l'EASI soient déployées conformément à la politique, aux directives et aux conditions de l'autorisation judiciaire pertinentes.

3.3.2. Fournir une assistance technique aux enquêtes sur la cybercriminalité visant à identifier les auteurs et à déterminer l'origine des attaques cybercriminelles en utilisant diverses méthodes, notamment la rétro-ingénierie des logiciels malveillants utilisés dans les attaques cybercriminelles afin de déployer des solutions techniques.

NOTE : Dans des circonstances exceptionnelles, tout opérateur de l'EASI peut déployer un OEE avec l'approbation de l'officier responsable au QG de l'EASI.

3.4. Conseiller en gestion de cas techniques (CGCT)

3.4.1. Les conseillers en gestion des cas techniques assurent la liaison entre les unités d'enquête et l'EASI. À ce titre, ils évaluent toutes demandes de services de l'EASI et contactent le sous-officier des opérations du QG de l'EASI lorsqu'une nouvelle demande de service justifie l'aide de l'EASI.

4. **Formation**

4.1. Opérateur de l'EASI

ébauche

4.1.1. Pour déployer une solution technique ou mener des activités de collecte de preuves, un opérateur de l'EASI doit avoir complété, avec succès, le programme de doublure de l'opérateur de l'EASI ou doit agir sous la supervision d'un opérateur de l'EASI certifié.

4.1.2. Veuillez contacter le QG de l'EASI à l'adresse RCMP.CAITHQ-EAISQG.GRC@rcmp-grc.gc.ca pour obtenir des informations sur le programme de formation des opérateurs de l'EASI.

5. **Services fournis**

5.1. L'EASI fournit des services aux partenaires nationaux et internationaux chargés de l'application de la loi, qui comprennent, entre autres, les activités suivantes :

Note : Conformément à la section 2.1, les activités suivantes ne peuvent être menées que par des opérateurs de l'EASI certifiés.

5.1.1. Le déploiement, la maintenance et le retrait discret d'OEE et d'autres solutions techniques qui nécessitent l'exploitation à distance, à proximité ou à accès rapproché de dispositifs et/ou de réseaux informatiques ;

5.1.2. Le déploiement, la maintenance et le retrait discret d'OEE et d'autres solutions techniques qui permettent de recueillir des preuves par des techniques d'accès à distance, proche ou rapproché ;

5.1.3. L'interception de communications par messagerie sécurisée ;

5.1.4. La localisation, l'identification et l'énumération de cibles et de dispositifs (par exemple, le balayage de services, les évaluations de vulnérabilité, l'identification d'infrastructures à distance, etc.)

5.1.5. L'Analyse du comportement des logiciels malveillants dans le but de déployer une solution OEE ou une autre solution technique.

6. **Demande d'assistance de l'EASI**

6.1. Pour initier une demande d'assistance de l'EASI, un conseiller en gestion de cas techniques (CGCT) du PGCT doit être consulté le plus tôt possible dans l'enquête afin de déterminer si une assistance peut être fournie. Il peut être joint par courriel à l'adresse RCMP.TCMP_HQ-PGDT_HQ.GRC@rcmp-grc.gc.ca.

6.2. Si le PGCT détermine que l'assistance de l'EASI peut être fournie au demandeur, les étapes suivantes doivent être complétées :

6.2.1. Remplir et soumettre le formulaire 6560, *Demande d'assistance - Équipe d'accès secret et d'interception (EASI)* http://infoweb.rcmp-grc.gc.ca/form/catalogue/6560f.pdf

6.2.2. Remplir et soumettre le formulaire 6505, *Demande d'action - OREC division à OREC division* http://infoweb.rcmp-grc.gc.ca/form/catalogue/6505f.pdf

6.2.3. S'assurer qu'une évaluation des risques a été effectuée ; et,

6.2.4. S'assurer qu'un protocole d'engagement est en place entre la DSET et l'équipe d'investigation.

ébauche

6.3. Une fois la demande approuvée, l'EASI collaborera avec un CGCT, l'unité requérante et toute autre unité des SET concernée pour fournir un soutien aux enquêteurs. Ce soutien peut inclure, sans s'y limiter, les éléments suivants :

6.3.1. Un examen des autorisations judiciaires avant qu'elles ne soient présentées aux tribunaux ;

6.3.2. Des recommandations sur la meilleure marche-à-suivre pour obtenir les meilleures preuves numériques possibles ;

6.3.3. Fournir des informations sur les solutions techniques secrètes ; et,

6.3.4. Fournir des conseils pour des solutions potentielles à des problèmes techniques d'enquête au fur et à mesure qu'ils se présentent.

6.4. Les politiques et les procédures décrites dans le présent chapitre s'appliquent lorsqu'une demande est reçue d'une agence autre que la GRC.

7. **Déploiement, maintenance et retrait des OEE**

7.1. Le DG SET approuvera le déploiement des OEE.

7.2. L'officier responsable SET approuvera le déploiement de toutes les autres solutions techniques.

7.3. Les OEE ne seront déployés, entretenus et retirés que par un opérateur de l'EASI certifié ou sous la direction d'un opérateur de l'EASI certifié, une fois que l'approbation du QG de l'EASI aura été reçue.

7.4. Les OEE sensibles ne seront déployés qu'à partir de l'environnement secret du QG de l'EASI, qui dispose des mesures de sécurité appropriées pour garantir la protection de la sensibilité de l'OEE et de la valeur probante des données recueillies.

7.5. Les OEE et/ou les autres solutions techniques qui nécessitent une couverture dans l'exécution des activités décrites dans la sec. 5 ne peuvent être acquis que par le biais du processus de dépenses sensibles (RO 581).

7.6. Les OEE et autres solutions techniques doivent être protégés en fonction de leur niveau de sensibilité. Une divulgation ou une compromission par inadvertance pourrait nuire gravement aux relations de la GRC avec ses partenaires et entraver considérablement la capacité de la GRC à enquêter sur des affaires graves.