**Leçon 3.x Renforcement des compétences en matière de cybercriminalité**

|  |  |  |
| --- | --- | --- |
| Leçon 3.x Renforcement des compétences en matière de cybercriminalité | | Durée: 130 minutes |
| **Ressources nécessaires :**   * PC/ordinateur portable chargé avec des versions de logiciel compatibles avec les matériaux préparés * Accès à Internet (si disponible) * PowerPoint ou autre logiciel de présentation | | |
| **Objectif de la session :**  L'objectif de cette session est de vérifier le niveau de compréhension des délégués sur les sujets présentés précédemment par l'analyse d'études de cas pratiques. | | |
| **Objectifs:**   * Analyser la synthèse des études de cas dans l'environnement de travail du groupe * Appliquer les connaissances acquises pendant la formation judiciaire de base sur la cybercriminalité et les preuves électroniques dans l'étude de cas * Rendre compte des conclusions de l'étude de cas * Comprendre quelles devraient être les prochaines étapes pour développer les connaissances et les compétences en matière de cybercriminalité | | |
| **Orientation des formateurs**  Au cours de la session, les sujets suivants doivent être pris en compte :   * Introduction à l'étude de cas * Division du groupe * Répartition du temps pour l'analyse * Répartition du temps pour le rapport du groupe * Étude de cas * Rapports des groupes * Réponses aux questions * Conclusions de l'exercice | | |
| **Contenu de la leçon** | | |
| **Numéros des Diapositives** | **Contenu** | |
| 1 à 3 | Les premières diapositives constituent l'introduction à la session et comprennent l'ordre du jour et les objectifs de la session. | |
| 4 à 7 | Ces diapositives présentent l'introduction à l'exercice lui-même avec de courtes explications sur les dispositions logistiques.  L'étude de cas est conçue de manière modulaire, ce qui signifie que différentes configurations de l'exercice peuvent être organisées. L'étude de cas est modulaire dans le sens où un, deux, quatre ou un nombre différent de groupes peuvent y travailler, selon les conditions. Chaque groupe, lorsqu'il y en a plusieurs, recevra sa partie de l'étude de cas et préparera sa partie du rapport d'étude de cas.  Idéalement, quatre groupes devraient être formés, et chaque groupe devrait recevoir sa partie de l'étude. Le groupe 1 devrait travailler sur les diapositives "Qui suis-je ?", le groupe 2 sur les diapositives "Suivez les données", le groupe 3 sur les diapositives "Suivez l'argent", et le groupe 4 sur les diapositives "Suivez le chef". Si le nombre de délégués est différent, l'expert doit adapter cette répartition.  A la fin de la session, tous les groupes qui font des rapports fusionneront en fait des rapports partiels en un seul grand rapport final, en réalisant que tous ont travaillé sur un seul cas et ont participé à la création d'un story board tout en résolvant le cas avec des conclusions communes.  En fonction des conditions de formation locales, l'expert devrait faire les ajustements nécessaires avec les délégués. Le synopsis détaillé de l'étude de cas est disponible comme matériel de formation supplémentaire.  Pour la version en ligne de la formation, l'étude de cas peut être organisée de manière à ce que les délégués appartiennent à un groupe pendant que l'expert les guide à travers les faits, les questions et les solutions, tout en s'engageant activement avec eux. | |
| 8 à 18 | Ces diapositives présentent un scénario d'étude de cas.  L'étude de cas est tirée d'une des situations réelles et toujours en cours dans l'une des parties à la Convention sur la cybercriminalité. Elle représente l'étude des nouvelles façons dont le blanchiment d'argent peut être organisé par l'utilisation abusive des médias sociaux, des systèmes de paiement en ligne et des systèmes de paris en ligne.  Toutefois, dans son essence, cette situation comprend des définitions et des termes déjà familiers d'accès illégal, d'interférence de données, de falsification informatique, de fraude informatique, d'infraction liée à des violations de droits d'auteur et de droits connexes du côté du droit matériel.  Sur le plan de la procédure, des outils tels que la conservation accélérée et la divulgation partielle des données relatives au trafic, l'ordonnance de production, la recherche et la saisie de données informatiques stockées, la collecte en temps réel de données relatives au trafic et l'interception de données relatives au contenu sont utilisés.  Le volet de l'entraide judiciaire utilise l'extradition, la conservation et la divulgation partielle accélérées des données relatives au trafic, la divulgation accélérée des données relatives au trafic conservées, l'entraide concernant l'accès aux données informatiques stockées, l'entraide concernant la collecte en temps réel des données relatives au trafic, l'entraide concernant l'interception des données relatives au contenu et les articles de la Convention de Budapest relatifs aux réseaux 24 heures sur 24 et 7 jours sur 7. | |
| 19 to 21 | Ces diapositives présentent les tâches, les problèmes et les questions possibles concernant l'étude de cas.  L'expert doit présenter les principaux problèmes qui représentent les idées principales du cas et qui doivent être explorées pendant le temps de travail en groupe.  Les questions principales couvrent tous les chapitres de la Convention sur la cybercriminalité. Les conclusions doivent être axées sur les actes criminels et les dispositions procédurales de demandes d’entraide pénales utilisées pour l'analyse du cas.  L'affaire n'est pas prête pour être jugée. | |
| 19 à 21 | Cette diapositive représente les questions et réponses spécifiques du groupe 1 concernant l'étude de cas.  Réponses :  - si aucun régime de rétention, l'article 16 suivi de l'article 18. Si un régime de conservation est en place, l'article 18 au réseau de médias sociaux concernant les données relatives au contenu. Contact avec le siège de la marque au sujet du jeu ;  - si aucun régime de conservation, article 16 suivi de l'article 18. Si un régime de conservation est en place, l'article 18 est transmis au réseau de médias sociaux concernant les informations de base sur l'abonné ;  - audition des témoins et vérification des comptes bancaires ;  - Article 8 ;  - identification des personnes qui administrent les pages primées et leur interrogatoire. | |
| 22 à 23 | Cette diapositive contient les questions et réponses spécifiques du groupe 2 concernant l'étude de cas.  Réponses :  - si aucun régime de rétention n’existe, l'article 16 suivi de l'article 18. Si un régime de conservation est en place, l'article 18 à l'ISP concernant les informations de base sur l'abonné, les données relatives au trafic et au contenu ;  - Adresses IP utilisées par l'administrateur des canaux, journaux d'activité de l'administration, journaux d'activité des utilisateurs concernant l'échange de données personnelles, autres preuves concernant le flux monétaire et la communication ;  - Les adresses IP obtenues en vertu des articles 16 et 18 seront reliées aux abonnés du PSI et à leurs contrats d'abonnement ;  - Article 19 sur les ordinateurs en possession des suspects, interrogatoire des suspects, déclarations des représentants des marques, des banques, des médias sociaux et des fournisseurs de services Internet et acquisition de données supplémentaires liées aux précédentes, identification du fournisseur de services hôte du marché noir dans le pays A, en fonction du chemin parcouru par les délégués sur le fournisseur du marché noir (son existence est-elle connue du fournisseur ou non), articles 16, 18 et 19, analyse des journaux d'activité des échanges entre vendeurs et acheteurs de données à caractère personnel et preuves supplémentaires à cet égard. Les articles 20 et 21 peuvent être utilisés pour la collecte et l'interception des données entre les vendeurs et les acheteurs de données privées à condition que leurs adresses IP soient identifiées ;  - La mise en œuvre de l'article 19 sur les ordinateurs suspects a montré la présence du contrôleur pour le logiciel malveillant troyen installé sur certains ordinateurs de la marque permettant l'accès aux canaux d'origine ;  - par les preuves électroniques acquises grâce à l'application de l'article 19 sur les ordinateurs des vendeurs et des acheteurs de données privées, qui montreront les relevés bancaires et le portefeuille électronique de crypto-monnaie ;  - les articles 2 et 4 concernant l'accès aux canaux originaux des médias sociaux de la marque et leur modification, les articles 7 et 10 concernant l'abus du jeu primé au nom de la marque et l'utilisation du logo de la marque et d'autres éléments des DPI. | |
| 24 | Cette diapositive présente les questions et réponses spécifiques du groupe 3 concernant l'étude de cas.  Réponses :  - enregistrement des données d'identification et des transactions monétaires ;  - oui, l'entreprise de paiement en ligne (OLPC) du pays B approuve la coopération volontaire. La demande doit donc être envoyée par les autorités du pays A conformément aux règles de l'entreprise ;  - Articles 29 et 31 pour la société de paiement en ligne concernant les comptes des utilisateurs, article 30 concernant les données relatives à la communication avec la société de paris en ligne du pays C (OLBC)  - Les articles 29 et 31 devraient être préparés pour le pays C également, étant donné qu'il n'approuve pas la coopération volontaire, tandis que l'article 26 peut être utilisé pour l'échange rapide d'informations entre les ALE.  - Les pays A, B et C peuvent organiser ensemble la mise en œuvre des articles 33 et 34 entre les utilisateurs des comptes OLPC du pays A et des comptes OLBC du pays B | |
| 25 | Cette diapositive représente les questions et réponses spécifiques du groupe 4 concernant l'étude de cas.  Réponses :  - Propriétaire et utilisation du compte OLPC, journaux de transactions, journaux IP concernant la communication avec les comptes OLBC, journaux IP concernant la communication avec les banques du pays A, articles 29, 30 et 31 concernant le flux et l'échange de données antérieurs ;  - oui, puisque l'OLPC approuve la coopération volontaire, donc avant la mise en œuvre des articles, le BSI et certaines données de trafic peuvent être recherchées ;  - Le pays A se concentrera désormais sur les personnes qui reçoivent des paiements sur leurs comptes bancaires ;  - Le pays A revient maintenant aux articles 16, 18 et 19 concernant l'ordre des transferts d'argent de l'OLPC vers les banques locales, et si nécessaire, les articles 20 et 21 peuvent être utilisés pour les données relatives au trafic et au contenu entre les principaux coupables et les passeurs de fonds ;  - pour les médias sociaux, les articles 16 et 18 pour la vérification des anciens fichiers de renseignements bancaires, pour la voix sur IP, les articles 20 et 21 ;  - L'étude de cas est ouverte, l'article 26 doit être utilisé et si les délégués veulent demander l'arrestation du principal suspect dans le pays E et l'extradition, l'article 24 peut être utilisé. | |
| 28 à 31 | Des diapositives qui introduisent et suivent les rapports de groupe. | |
| 31 à 33 | Les dernières diapositives permettent au formateur de revoir les objectifs d'apprentissage avec le public afin qu'il puisse s'assurer qu'ils ont été atteints. C'est également l'occasion pour les délégués de soulever les questions qui pourraient être en suspens ou pour lesquelles ils n'ont pas bien compris les sujets présentés.  En outre, le formateur peut utiliser la session pour vérifier les connaissances acquises en posant des questions aux participants. Ceci est important car il n'y a pas d'évaluation formelle pour le cours. | |
| **Exercices pratiques**  Une étude de cas est envisagée dans cette leçon. | | |
| **Évaluation/vérification des connaissances**  Aucune vérification ou évaluation des connaissances n'a été demandée pour cette session. | | |