**Plan de la session**

Session 2.1.3 (Technologie)

|  |  |  |
| --- | --- | --- |
| Session 2.1.3 (Technologie) | | Durée : 150 Minutes |
| **Ressources nécessaires:**   * PC/ordinateur portable sur lequel sont installées des versions logicielles compatibles avec les matériels préparés. * Projecteur et écran mural. * Accès à Internet (si possible). * Papiers et stylos pour les participants. | | |
| **Objectif de la session:**  L'objectif de cette session est de donner aux participants des informations actualisées sur les nouveaux types de criminalité et de menaces résultant de l’utilisation des nouvelles technologies. Certains sujets qui ont été brièvement abordés dans le cours d'introduction seront étudiés plus en détail au cours de cette session. | | |
| **Objectifs:**  Au terme de la présente session, les participants pourront :   * Expliquer les différentes formes de compromission de la messagerie d’entreprise (CME) * Identifier les menaces posées par l'internet des objets (IdO) * Faire la distinction entre les différentes couches de l'internet * Expliquer comment sont effectuées les transactions en monnaies virtuelles | | |
| **Indications destinées au formateur**  Cette session a pour but de présenter les nouvelles technologies qui ont une incidence sur le comportement criminel. L'évaluation des menaces que représente la criminalité sur internet (IOCTA) 2017, qui a été publiée en septembre 2017, est citée dans certaines diapositives car ce rapport contient les informations les plus récentes disponibles dans ce domaine. Il appartiendra aux formateurs de les actualiser au fur et à mesure de la publication de nouveaux rapports et de nouvelles données. Les vidéos utilisées lors de cette session sont publiques et peuvent être téléchargées gratuitement et utilisées. Le formateur peut choisir de faire des démonstrations pour illustrer son propos. Il pourrait, par exemple, présenter le navigateur TOR lors de la session sur le *darknet* pour montrer aux participants comment accéder aux outils de la cybercriminalité en ligne. | | |
| **Contenu de la session** | | |
| **Numéros des diapositives** | **Contenu** | |
| 1 à 3 | Les premières diapositives définissent la structure et les objectifs de cette session. Les participants auront la possibilité de poser des questions préliminaires sur ces deux points. | |
| 4 à 18 | Ces diapositives donnent des informations sur l'influence de l'internet dans le monde (diapositives 5 à 12) et dans le pays où le cours est dispensé (diapositives 13 à 18). Le formateur doit veiller à ce que ces diapositives correspondent à la situation du pays où le cours est dispensé et à les utiliser pour examiner l'impact de l'internet au niveau national et mondial. | |
| 19 à 30 | Ces diapositives fournissent des renseignements sur des crimes récents qui ont eu un retentissement important. Le formateur devrait se familiariser avec les crimes commis et présenter ceux qui sont pertinents pour la région où la formation est dispensée. Il souhaitera peut-être les remplacer par des cas qui se sont produits dans le pays en question. | |
| 31 à 32 | A pour but de présenter des informations publiées par l'IOCTA 2017 sur les attaques commises contre les messageries d’entreprise (compromission de la messagerie d’entreprise ou CME). | |
| 33 | Le formateur doit demander aux participants de répondre à la question posée dans la diapositive. S'il n'y a pas de réponse, le formateur poursuit sa présentation. Si des participants citent des exemples, le formateur leur donnera du temps pour qu’ils les présentent en détail et comparera les informations communiquées à celles qui figurent dans la présentation | |
| 34 à 42 | Ces diapositives et les vidéos connexes, qui proviennent de Trend Micro/Europol, expliquent très bien les méthodes utilisées pour prendre le contrôle d’une messagerie d'entreprise (CME) ainsi que les mesures visant à les prévenir. La vidéo finale présente la prise de contrôle et la manipulation de certains processus internes à l’entreprise, qui est une variante de la compromission de la messagerie d’entreprise. | |
| 43 à 44 | Il s'agit d'une introduction à l'internet des objets (IdO). Il serait bon que le formateur invite les participants à faire part de leurs connaissances ou expériences éventuelles dans ce domaine.  Il est à noter que la diapositive 45 est une vidéo qui donne un très bon exemple de la façon dont un véhicule automobile peut être connecté à plusieurs services par IdO et qui montre les avantages de ces services pour le client. Le formateur peut également réfléchir à la disponibilité des preuves électroniques qui peuvent résulter de ces connexions. | |
| 45 | Cette vidéo donne un très bon exemple de la façon dont un véhicule automobile peut être connecté à plusieurs services par IdO et montre les avantages de ces services pour le client. Le formateur peut également réfléchir à la disponibilité des preuves électroniques qui peuvent résulter de ces connexions. | |
| 46 | Cette diapositive permet de présenter la version IP 6, qui est une plateforme pour l’IdO. | |
| 47 | Cette diapositive donne au formateur la possibilité d’examiner les questions de sécurité liées aux « appareils connectés » (IdO) et de faire remarquer que leurs fabricants ne sont pas des experts en matière de sécurité. Les « appareils connectés » sont une bombe à retardement. Le formateur souhaitera peut-être développer les différents points cités en fonction de sa propre connaissance du sujet. | |
| 48 à 49 | Ces diapositives présentent des informations récentes publiées dans le rapport IOCTA 2017. Elles viennent éclairer les questions soulevées dans la diapositive 20. | |
| 50 à 57 | Ces diapositives fournissent des informations sur les « appareils connectés » et certaines des questions connexes. Les formateurs sont encouragés à utiliser des exemples qu'ils connaissent, en particulier s'il s’agit de problèmes de sécurité, comme c'est le cas avec iKettle, une bouilloire connectée au wifi. | |
| 58 à 60 | Ces diapositives marquent le début de la session sur le *darknet* et les services connexes. Elles reprennent des informations publiées dans le rapport de l'IOCTA qui permettent de placer le sujet dans son contexte et de le développer. | |
| 61 à 67 | Ces diapositives expliquent l'utilisation criminelle du *darknet* et des services offerts sur ce réseau et présentent des exemples réussis de fermeture de sites exploités à des fins criminelles. Le formateur est encouragé à montrer en direct comment accéder au *darknet*, s’il y a lieu et s’il existe une connexion internet appropriée. | |
| 68 à 77 | Ces diapositives sont un rappel des questions soulevées dans le cours d'introduction ; elles sont complétées par une vidéo et présentent, comme pour d’autres sujets, les informations les plus récentes contenus dans le rapport IOCTA 2017. | |
| 78 à 79 | Le formateur devrait récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives aux sujets abordés dans cette leçon. | |
| **Exercices pratiques**  Il n'y a pas d'exercices pratiques obligatoires mais le formateur est encouragé à faire une démonstration en direct de l'accès au darknet, le cas échéant. | | |
| **Évaluation/Vérification des connaissances**  Aucune évaluation formelle n'a été préparée pour cette session. Le formateur compte sur une participation active des participants. | | |