MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

La MInute Cyber 11

MOOC SENSY-CRISE

Face à l'augmentation des cyberattaques, les TPE, PME et collectivités territoriales sont en première ligne. En 2023, 43 % des cyberattaques en France ciblaient ces structures, entraînant des conséquences graves : pertes financières, interruptions d'activité, voire fermetures définitives*. Ces organisations, souvent dépourvues de services informatiques dédiés, manquent de préparation face à ces menaces croissantes. Pour combler ces lacunes, le commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI), en partenariat avec cybermalveillance.gouv.fr, a développé le MOOC SenCy-Crise, un enseignement gratuit, conçu pour être accessible à tous.

Depuis son lancement en juillet 2024, ce programme d'e-sensibilisation a déjà été consulté par plus de 20 000 utilisateurs. Il propose des outils pratiques pour anticiper, gérer et tirer des enseignements des crises cyber. Récompensé par le premier prix lors du concours vidéo « Racontez votre projet en 80 secondes », organisé dans le cadre des Trophées MInnov par la Mission Innovation, Simplification et Transformation (MIST) du ministère de l'Intérieur, SenCy-Crise a été salué pour son impact et son utilité. Ce prix met en avant une initiative structurante qui répond aux besoins urgents des petites et moyennes structures, souvent en manque de solutions adaptées.

Le MOOC SenCy-Crise s'articule autour de trois modules pratiques pour accompagner chaque étape d'une crise :

- Avant la crise : prévenir et anticiper. Identifier les menaces et établir des plans d'action adaptés pour renforcer la sécurité.
- Pendant la crise : réagir et résister. Adopter les bons réflexes pour minimiser les impacts d'une attaque en cours.
- Après la crise : capitaliser et se renforcer. Tirer des leçons des incidents pour améliorer sa résilience face à de futures menaces.

Cette approche pédagogique repose sur des vidéos interactives, des témoignages d'experts et de victimes, ainsi que des outils téléchargeables. En seulement deux heures de formation, les utilisateurs, qu'ils soient dirigeants de PME, responsables de collectivités ou membres d'associations, acquièrent des compétences concrètes pour gérer une crise de bout en bout. Accessible même aux non-spécialistes, le programme s'adapte au rythme de chacun et contribue à réduire les vulnérabilités face aux cyberattaques. Une étude Ipsos réalisée pour cybermalveillance.gouv.fr souligne l'urgence de cette sensibilisation : 61 % des Français ont été victimes d'un acte de cybermalveillance en 2023, mais une majorité peine à réagir efficacement. Le MOOC comble ce déficit en apportant une réponse claire et pragmatique.

Lors du concours MInnov, SenCy-Crise s'est imposé face à des projets prestigieux, tels que l'exosquelette EXO-M du GIGN ou les drones automatisés du SDMIS. Avec plus de 150 000 vues et 7 500 réactions sur LinkedIn pour les vidéos en compétition, ce projet a mobilisé un large public et démontré son potentiel. Le MOOC fut d'ailleurs doublement primé, car ayant remporté le 25 novembre dernier le 1er prix dans la catégorie Projets / Initiatives - Équipes Cyber et organisations publiques lors de la CYBERNIGHT 2024.

Plus qu'un outil, SenCy-Crise est un levier de résilience collective face aux cybermenaces. Son succès dépasse le cadre du trophée en sensibilisant des milliers d'organisations à travers la France. En renforçant la culture de la cybersécurité, il contribue activement à protéger le tissu économique, associatif et institutionnel.

Pour découvrir et commencer le MOOC SenCy-Crise, rendez-vous sur :

https://www.cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

**Chiffre ANSSI – Panorama de la cybermenace 2023*

FORMATION DÉLIVRÉE DANS LES BALKANS

Du 13 au 15 novembre, le COMCYBER-MI était présent dans les Balkans. Pendant 3 jours, le Général de brigade Patrick Perrot et Mme Ysens de France ont proposé aux forces de police locales, une formation sur mesure dédiée aux enjeux de l'Intelligence Artificielle (IA).

À l'invitation du Western Balkans Cyber Capacity Center, ces deux experts ont présenté les capacités opérationnelles de l'IA dans le champ de la sécurité intérieure incluant l'espace cyber, les enjeux réglementaires avec l'AI act de l'UE & la Convention AI du Conseil de l'Europe, la nécessaire appropriation scientifique, les questionnements sociétaux préalables et l'impérieuse question de la bonne gouvernance pour y répondre à travers la présentation d'une feuille de route concrète. La mise à disposition de ce savoir-faire #IA dans ce centre de formation dédié à la cyber sécurité et à la cyber criminalité, contribue à répondre à l'impératif de lutter ensemble contre une criminalité sans frontière avec une compréhension partagée des outils qui l'alimente et peut la combattre.

LA PREUVE NUMÉRIQUE AU CŒUR DES ENQUÊTES JUDICIAIRES

De l'aveu aux témoignages sans oublier l'ADN, au cours d'une enquête judiciaire, plusieurs preuves peuvent être recueillies et exploitées afin de démontrer la culpabilité ou l'innocence d'un suspect. Parmi celles-ci, la preuve numérique occupe une place de plus en plus prépondérante considérant la transformation numérique en cours au sein de notre société.

La preuve numérique n'est pas définie dans le Code de procédure pénale, la procédure pénale ne comportant pas d'ailleurs de théorie générale de la preuve. La preuve peut être définie comme le moyen permettant d'affirmer l'existence ou la non-existence d'un fait, le numérique pouvant être défini comme la représentation de l'information ou de grandeurs physiques par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1. Ainsi, la preuve numérique est indissociable des techniques d'enquête numériques. Sans prétendre à l'exhaustivité, les techniques d'enquête numériques ne cessent de croître : écoutes téléphoniques, géolocalisations, perquisitions informatiques, enquêtes sous pseudonyme, accès aux correspondances stockées, captation des données informatiques. Cette extension des techniques s'explique par un intérêt pénal de plus en plus marqué pour cette preuve si particulière.

Par essence fragile et volatile, la preuve numérique est singulière au regard de son recueil, potentiellement très intrusif. Portant sur des données à caractère personnel, les techniques d'enquête numériques impliquent nécessairement une ingérence dans les droits fondamentaux des suspects et des victimes d'une infraction. Dès lors, le Code de procédure pénale prévoit plusieurs garanties permettant de fonder ou non une investigation :

- la gravité de l'infraction suspectée est très souvent imposée. La loi prévoit différents seuils (3 ans, 5 ans d'emprisonnement encourus) ou des périmètres infractionnels spécifiques (criminalité et délinquance organisées). *A contrario*, certaines techniques comme les perquisitions informatiques échappent à cette date à toute exigence de gravité.
- la durée de la mesure d'investigation est parfois limitée dans le temps et dans l'espace. Certaines ne peuvent excéder 8 jours (géolocalisation) quand d'autres sont limitées à un mois, renouvelable une fois (interception de correspondances).
- la mise en œuvre d'une technique d'enquête numérique est quasi systématiquement soumise à une autorisation préalable délivrée soit par le procureur de la République, soit par le Juge des libertés et de la détention. L'intensité du contrôle varie toutefois en fonction de la typologie des investigations mises en œuvre.

Enfin, la preuve numérique implique nécessairement une certaine technicité pour son recueil et son exploitation. En effet, soumise aux lois de l'informatique, sa fragilité et sa volatilité impliquent que les enquêteurs soient formés à sa manipulation. Formations initiale et continue des enquêteurs, acquisition et déploiement de matériels spécifiques sont le corolaire de cette mission particulièrement sensible.

Pour aller + loin...

MonAideCyber

Le mois dernier, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) annonçait le lancement de MonAideCyber. Gratuit, ce dispositif vise à accompagner les entités publiques, les associations et les entreprises dans une première démarche de sécurisation informatique. Celles-ci sont tout d'abord mises en relation avec un « Aidant cyber ». Il s'agit de tiers de proximité, outillés voire formés par l'ANSSI, engagés sur la base du volontariat. Ce sont notamment des représentants de services de l'État (police, gendarmerie, agences régionales de santé, etc.), de collectivités, de groupements d'intérêt public, d'associations et de sociétés privées. L'Aidant cyber réalise ensuite un diagnostic de premier niveau, d'une durée d'1h30, puis oriente l'usager vers des dispositifs complémentaires locaux. Ce diagnostic préconise 6 mesures de sécurité prioritaires à mener sur les 6 prochains mois. Véritable levier permettant de tirer vers le haut le niveau de maturité cyber d'une entité, MonAideCyber succèdera prochainement à Di@GoNal dont il s'est inspiré pour construire un produit au plus près des attentes du terrain.

Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 011 - NOVEMBRE 2024

Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : GBR P. PERROT - LCL S. LAMBERT - CEN D. MALET - CEN M. AUDIBERT
Conception graphique et maquettage : Mme M. BARREAU

En attendant le prochain numéro de La MInute cyber, suivez notre actualité :

sur LinkedIn et sur X (ex-Twitter) : ***@ComCyberMI***