La MInute Cyber 10

©RÉPUBLIKGROUP-IT

MISE EN LUMIÈRE DE L'ACTION DU DÉPARTEMENT PRÉVENTION ET CYBER-RÉSILIENCE DU COMCYBER-MI

Le 2 septembre 2025, la révélation d'une attaque cyber, ayant touché un grand constructeur automobile britannique, mettait en lumière le fait que les impacts de ce type d'attaque pouvaient s'avérer colossaux. En l'espèce, l'entreprise concernée avait été obligée de fermer ses systèmes et ses lignes de production pendant plus d'un mois, provoquant une perte hebdomadaire de 50 millions de livres, à laquelle devraient s'ajouter les pertes de l'ensemble des fournisseurs du constructeur pour obtenir une vision plus exacte de l'ampleur des dégâts. De plus, le gouvernement britannique avait dû intervenir, via une garantie de prêt, pour soutenir la plus grande entreprise du secteur automobile britannique, composée en grande partie de PME et employant plus de 100 000 personnes[1].

Le caractère systémique des attaques informatiques, qui touchent tant les organisations privées que publiques, mais aussi tous les pans de l'économie et de la société, associé à l'ampleur qu'elles peuvent revêtir, implique le fait qu'il faille désormais mettre en œuvre une démarche de cyber-résilience. La résilience assurant le maintien des activités essentielles de l'organisation en cas de perturbation ou d'incident majeur[2].

Cette démarche passe notamment par la réalisation régulière de cyber stress tests, autrement dit des exercices de gestion de crise d'origine cyber (GCC), indispensables au bon entraînement des organisations, en les engageant dans un processus d'amélioration continue : entraînement des équipes par l'accoutumance à ce type de situations (stress, capacités de coordination et de montée en puissance) ; évaluation des plans de continuité et de reprise d'activité, des stratégies de communication, de différentes clauses contractuelles et assurantielles, etc.

Pleinement engagé dans l'amélioration de la cyber-résilience de la Nation, le Département Prévention et Cyber-Résilience du COMCYBER-MI contribue activement à l'entraînement des forces vives de la Nation, publiques ou privées, pour faire face aux nouveaux défis du cyberespace.

Tout d'abord en participant régulièrement à des exercices de GCC tels que REMPAR 25 aux côtés de l'entreprise française Outscale, ou encore en renforçant l'Institut des Hautes Etudes du Ministère de l'Intérieur lorsque celui-ci en organise.

Ensuite, en co-construisant ces exercices avec des partenaires, tels que l'association d'élèves de Sciences Po Paris *« Défense et Stratégie »*, Guardia Cybersecurity School Paris, l'INSA Centre Val de Loire, entre autres.

Enfin, en se déplaçant partout en France pour sensibiliser des acteurs aussi variés que des préfectures, collectivités territoriales, TPE-PME aux bonnes pratiques en matière de préparation à la gestion de crises, en amont des exercices qu'ils souhaitent effectuer.

**Avec son MOOC SenCy-Crise le COMCYBER-MI a vu ces actions de prévention récompensées dès 2024 (photo d'illustration).*

1. https://www.lefigaro.fr/flash-eco/cyberattaque-reprise-partielle-de-la-production-chez-jaguar-land-rover-20251007
2. https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

Quand un simple appel téléphonique déclenche un vol massif de données personnelles

En 2025, des dizaines d'entreprises dans le monde ont été victimes du groupe de pirates ShinyHunters. Leur cible : les données clients stockées dans l'une des principales plateformes de gestion de la relation client. Mais au lieu de forcer des systèmes complexes, les pirates ont utilisé une méthode bien plus simple : la tromperie humaine.

Concrètement, les attaquants appelaient des employés en se faisant passer pour le support technique. Ils leur demandaient de saisir un code sur la page officielle de la plateforme. Derrière ce geste en apparence anodin se cachait un piège : ce code permettait aux pirates d'obtenir un jeton d'accès (OAuth), véritable passe-partout numérique. Avec lui, l'attaquant pouvait entrer dans les systèmes des entreprises et copier des millions de données clients et professionnelles. Dans d'autres cas, les pirates profitaient d'intégrations tierces (des outils connectés à la plateforme, à l'instar d'un chatbot utilisant l'intelligence artificielle). Ces connexions mal sécurisées leur ouvraient les portes des bases de données. Résultat : le groupe de pirates affirme avoir volé plus d'1,5 milliard d'enregistrements auprès de 760 entreprises.

Cette affaire rappelle que la cybersécurité ne repose pas seulement sur des logiciels. Le maillon humain reste souvent la cible privilégiée. Pour se protéger, les organisations doivent former leurs équipes, limiter les autorisations, surveiller les accès inhabituels et révoquer rapidement tout jeton suspect.

GLOSSAIRE

- **Ingénierie sociale :** technique de manipulation psychologique visant à tromper une personne plutôt qu'un ordinateur.
- **Vishing :** fraude par téléphone, proche du *phishing* par e-mail.
- **OAuth / jeton d'accès :** clé numérique qui autorise une application à accéder aux données d'un utilisateur sans demander son mot de passe.
- **Intégration tierce :** application ou service externe connecté à une plateforme principale (par exemple, un outil d'e-mail relié à la plateforme de gestion de la relation client).
- **Chatbot IA :** logiciel qui interagit avec un humain *via* un langage écrit.
- **Exfiltrer des données :** voler et transférer discrètement des informations hors du système.

Intervention du général HUSSON au Forum InCyber Canada

L'attaché de sécurité intérieure au Canada, le colonel Frédéric Brachet, a accueilli le général de division Christophe Husson lors de son déplacement au Canada, qui a eu lieu du 14 au 16 octobre 2025.

Le chef du COMCYBER-MI était présent au Forum InCyber Canada, qui se tenait à Montréal, événement et lieu de rencontre de la communauté mondiale de la cybersécurité. En effet, des délégations de plus de 35 pays, issues des structures publiques et privées de tous secteurs, étaient ainsi représentées et échangeaient durant cet événement bilingue (intégralement traduit en anglais et en français).

Le général Husson a pu présenter le COMCYBER-MI, ses missions, modes d'action, son environnement, et les enjeux auxquels il fait face, au cours d'une table-ronde dénommée *« Puissance cyber : regards croisés des nations »*, aux côtés de responsables cyber de structures étatiques des Etats-Unis, de Belgique, de Lituanie et du Canada, mais aussi d'universitaires et de chefs d'entreprises.

Ce déplacement concourait également à entretenir les échanges et à partager les bonnes pratiques, que ce soit lors de la visite auprès des services cyber de la police de Montréal ou de la Sûreté du Québec.

Enfin, le général Husson a pu s'entretenir avec monsieur, Stéphane Le Bouyonnec, sous-ministre du ministère québécois de la Cybersécurité et du Numérique, s'agissant des perspectives de renforcement de la coopération bilatérale en matière de lutte contre la cybercriminalité.

POUR ALLER + LOIN…

Octobre 2025 : 13e édition du Cybermois

La 13e édition du Cybermois se déroulait des 1er au 31 octobre.

Ce rendez-vous, dénommé le Mois européen de la cybersécurité (European Cybersecurity Month), a été créé en 2012, à l'initiative de l'Agence de l'Union européenne pour la cybersécurité (ENISA).

Décliné en France sous le nom « Cybermois », il est piloté par le dispositif national Cybermalveillance.gouv.fr ; ce dernier ayant pour missions la sensibilisation, la prévention et l'assistance aux victimes d'actes de cybermalveillance.

Durant tout le mois d'octobre, des activités étaient ainsi organisées sur la France entière (CyberTour de France) et en Europe autour des enjeux de cybersécurité. Nombreux acteurs publics, privés et associatifs se mobilisaient pour proposer un programme pédagogique, à destination de tous les publics et aux formats variés (des événements ou des vidéos, par exemple).

L'édition 2025 du Cybermois proposait un angle original, « Histoire de Cyber », une campagne de sensibilisation revisitant des faits historiques emblématiques pour illustrer, avec pédagogie, les bonnes pratiques à adopter en matière de cybersécurité. Napoléon, Marie-Antoinette ou Christophe Colomb sont ainsi devenus les personnages d'affiches au ton décalé.

Le Commandement du Ministère de l'Intérieur dans le cyberespace s'est pleinement mobilisé durant cette campagne. Il a ainsi diffusé des fiches cyber sur ses réseaux sociaux, invitant aux bonnes pratiques. Il a également réalisé et diffusé des affiches déclinant le thème « Histoire de Cyber ». L'une d'elle évoquait les cybermenaces en lien avec l'Intelligence Artificielle via l'opération Fortitude. Une autre mettait en avant l'importance de sécuriser ses mots de passe, en prenant l'exemple de la machine Enigma. D'autres médias étaient utilisés. Un reportage sur l'histoire des Taxis de la Marne, réalisé dans la commune de Gagny, illustrait l'importance de maintenir ses appareils numériques et logiciels en condition, mais aussi d'effectuer les mises à jour. Également, la création d'un motion design, narrant la célèbre affaire du « collier de la Reine », était l'occasion de sensibiliser au risque de hameçonnage et de donner des conseils pour s'en prémunir.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 10 - OCTOBRE 2025
Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : CEN M. ROUSSEAU - CEN N. PETITPAS - SecCyber
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