MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*

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

La MInute Cyber 09



DONNÉES COMPROMISES : UN RISQUE QUI S'INSCRIT DANS LA DURÉE

Lorsqu'une fuite de données est découverte, l'attention se porte naturellement sur l'incident lui-même. Pourtant, le risque ne disparaît pas une fois la compromission identifiée. Les informations exposées peuvent continuer à être exploitées pendant des semaines, des mois, voire davantage.

Nom, prénom, adresse mail, numéro de téléphone, coordonnées professionnelles ou informations administratives / bancaires peuvent être recoupés avec d'autres éléments disponibles en ligne ou issus de précédentes compromissions. Pris isolément, ces renseignements peuvent sembler anodins. Mis bout à bout, ils permettent pourtant de construire des sollicitations beaucoup plus crédibles et personnalisées.

C'est là que réside l'un des principaux risques pour les particuliers. Les cybercriminels peuvent exploiter le contexte d'une fuite pour adresser de faux messages de vérification, de sécurisation de compte, de remboursement ou de mise à jour. Ils peuvent également reprendre le nom de l'organisme concerné ou utiliser des informations personnelles exactes afin de renforcer la vraisemblance de leur démarche.

Un message contenant des données justes n'est donc pas nécessairement authentique.

Dans les semaines et les mois qui suivent une compromission, la vigilance doit rester de mise face aux sollicitations inattendues, notamment lorsqu'elles invitent à cliquer sur un lien, communiquer des informations personnelles, modifier un mot de passe ou effectuer une démarche dans l'urgence.

Le bon réflexe consiste à ne pas agir directement depuis le message reçu. En cas de doute, mieux vaut rejoindre par ses propres moyens le site ou l'application officielle de l'organisme concerné, ou utiliser ses coordonnées habituelles. Les informations diffusées par les organismes concernés peuvent également permettre aux usagers de mieux identifier les démarches légitimes et de repérer plus facilement les tentatives frauduleuses.

Une donnée compromise ne cesse pas d'être sensible lorsque l'incident est clos. Elle peut être conservée, recoupée et réutilisée longtemps après la fuite initiale. La compromission n'est donc pas seulement un événement ponctuel : elle peut devenir la matière première d'une nouvelle attaque.

Anticiper cette seconde phase, c'est limiter la capacité des cybercriminels à transformer une fuite en opportunité.

Le Cyber Resilience Act (CRA)

Le CRA est le règlement européen qui renforce la cybersécurité des produits comportant des éléments numériques mis à disposition sur le marché de l'Union : logiciels, matériels, objets connectés et, dans certains cas, solutions de traitement de données à distance liées au produit. Son ambition : réduire les failles dès la conception, mieux les traiter pendant toute la durée de vie du produit et donner aux utilisateurs une information plus claire sur les mises à jour de sécurité.

Le règlement est entré en vigueur le 10 décembre 2024. Depuis le 11 septembre 2026, une première obligation s'applique déjà : les fabricants doivent signaler les vulnérabilités activement exploitées et les incidents graves ayant une incidence sur la sécurité de leurs produits. La déclaration s'effectue via la plateforme européenne de l'ENISA. Elle comprend une alerte sous 24 h, une notification plus complète sous 72 h, puis un rapport final : au plus tard 14 jours après la mise à disposition d'une mesure corrective pour une vulnérabilité, ou dans le mois suivant la notification d'un incident grave. En France, le CERT-FR est le CSIRT coordinateur.

Les principales obligations de fond s'appliqueront à partir du 11 décembre 2027 : sécurité dès la conception, gestion des vulnérabilités, mises à jour pendant la période de support, documentation technique, évaluation de conformité et apposition du marquage CE lorsque les exigences sont respectées.

Le CRA concerne d'abord les fabricants, mais aussi les importateurs et les distributeurs. Les utilisateurs devraient ainsi bénéficier de produits plus sûrs, de correctifs mieux suivis et d'une information accrue sur les risques.

CyberNight 2026

Hier, au sein du Théâtre Mogador, a eu lieu la cérémonie de remise des Trophées de la CyberNight 2026.

Pour le COMCYBER-MI, tout a commencé le 8 septembre dernier, par la présentation de son MOOC « Cap Cyber crises & collectivités », exercice de simulation en ligne innovant destiné aux élus. Fruit dune coopération avec l'Association des maires de France et des présidents d'intercommunalité (AMF) et le Centre d'Analyse et de Lutte contre les Atteintes aux Élus (CALAE), ce module de formation en ligne adopte une approche immersive. Son but : permettre aux élus locaux et à leurs agents de se confronter à des situations réalistes de crise cyber, et ainsi de développer les bons réflexes en amont. Il se compose d'une formation théorique avec des fiches pratiques, de témoignages de collectivités, d'un jeu de rôle évolutif, et de conseils pratiques du CALAE. Durant trois minutes, nos experts du Département Prévention et de la Cyber Résilience (DPCR) se sont donc attachés à convaincre un jury d'une trentaine de membres, spécialistes de la cybersécurité mais aussi des questions de sécurité globale et de sûreté.

Lors de cette sixième édition, le COMCYBER-MI, engagé dans la catégorie « Défense, cyber défense, et protection des entités publiques », a donc remporté XXX. Devant plus de mille professionnels, les personnels du COMCYBER-MI, aux côtés de M. le commissaire divisionnaire Eric Levy-Valensi, adjoint du général de division Patrick Touak, ont ainsi vu leur engagement, mais aussi celui de leurs partenaires, récompensé. C'est aussi la mobilisation au quotidien de nombreux acteurs, publics ou privés, engagés dans la lutte contre les cybermenaces, qui fut mise à l'honneur à travers cette récompense.

Un grand bravo à nos lauréats !

POUR ALLER + LOIN...

Des humains peuvent lire certaines conversations ChatGPT

Des conversations que vous pensiez privées peuvent être examinées par des prestataires chargés d'évaluer ChatGPT, en l'occurrence par des humains travaillant pour OpenAI ; une pratique que l'entreprise américaine d'intelligence artificielle n'a pas clairement signalée aux utilisateurs concernés. Cette pratique s'inscrit notamment dans un dispositif interne baptisé « Project Lily », qui ferait appel à des prestataires chargés d'évaluer des conversations réelles afin d'améliorer la qualité des réponses du chatbot.

Ces conversations soumises à cette évaluation sont présentées aux annotateurs après des mesures de protection visant notamment à limiter les informations personnelles. Les évaluateurs analysent les réponses produites par ChatGPT, les comparent et peuvent justifier leur appréciation. L'objectif est notamment d'identifier les erreurs, les comportements indésirables ou les formulations problématiques afin d'améliorer les futurs modèles. Cette révélation pose surtout la question du niveau réel de confidentialité des échanges avec ChatGPT. Même si l'accès humain est limité et encadré, une conversation saisie dans un service grand public ne doit donc pas être considérée comme une correspondance strictement privée.

OpenAI confirme officiellement qu'un nombre limité de collaborateurs autorisés et de prestataires de confiance peut accéder à certains contenus, dans des circonstances précises : amélioration des modèles, sécurité, assistance aux utilisateurs ou questions juridiques. L'entreprise indique que ces accès sont contrôlés et soumis à des obligations de confidentialité. Les utilisateurs disposent toutefois de paramètres de confidentialité permettant de refuser l'utilisation de leurs conversations pour améliorer les modèles. Pour les services grand public comme ChatGPT, OpenAI indique que les contenus peuvent être utilisés pour entraîner ses modèles, sauf désactivation de cette option.

À retenir : le fait qu'un humain puisse potentiellement examiner une conversation constitue donc un enjeu réel. Il est donc préférable de ne pas transmettre à ChatGPT des informations particulièrement sensibles que l'on ne souhaiterait pas voir accessibles.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 09 - SEPTEMBRE 2026
Directeur de la publication : GDI P. TOUAK
Responsable éditorial : CEN D. MALET
Rédacteurs : LCL. S. LAMBERT - CEN D. MALET - LTN. M. FISSEAU
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