BULLETIN DE VEILLE CYBER

11 février 2025

EDITION N°11

L'ANSSI ÉMET DES RECOMMANDATIONS POUR SÉCURISER LES SYSTÈMES D'IA

[10 FEVRIER 2025] - Dans le cadre du Sommet pour l'IA, qui a lieu cette semaine à Paris, l'ANSSI a publié un rapport présentant les principaux scénarios de compromission de ces systèmes et les conseils pour atténuer les risques. Le document a été cosigné par les agences nationales de cybersécurité de 16 pays, dont celles du Royaume-Uni, du Canada, de l'Allemagne et de la Corée du Sud.

Elle recommande de cartographier l'ensemble de la supply chain, qu'il s'agisse des composants matériels et logiciels et des jeux de données, Elle demande aux entreprises de promouvoir les bonnes pratiques de cybersécurité, en valorisant la réglementation.

Source : https://www.usine-digitale.fr/article/cybersecurite-l-anssi-fournit-plusieurs-recommandations-pour-securiser-les-systemes-d-ia.N2227231

LE PROTOCOLE D'ALERTE ZATAZ, VERSION 2025

[8 FEVRIER 2025] - Le protocole d'alerte ZATAZ a fêté ces 25 ans.
Le protocole d'alerte ZATAZ permet de signaler les failles de sécurité, les fuites de données et les cyberattaques auprès des entreprises, associations, institutions et sites gouvernementaux.

Ce protocole est totalement gratuit, agit en toute indépendance, transparence et dans un cadre strictement éthique. En 25 ans, le PAZ (le Protocole d'Alerte ZATAZ) a déjà pu aider plus de 80 000 entreprises.

L'objectif principal du protocole d'alerte ZATAZ est de réduire les risques de cybersécurité en informant rapidement les entités concernées. Grâce à un système structuré et transparent, les sources, victimes et partenaires peuvent suivre en direct l'évolution des signalements et leur traitement. Le PAZ a signé sa 81 480ème alerte en ce 07 février 2025.

Source : https://www.zataz.com/le-protocole-dalerte-zataz-version-2025/

LA MÉTROPOLE DU GRAND PARIS DÉPLOIE UN PROGRAMME DE SOUTIEN AUX COMMUNES

[7 FEVRIER 2025] - Pour soutenir les communes confrontées aux attaques la Métropole du Grand Paris lance un programme d'accompagnement des 130 communes qu'elle regroupe. Ce programme est conduit en partenariat avec le Campus Cyber, dans le cadre du dispositif CYBIAH (Cybersécurité et Intelligence Artificielle Hub).

Les communes sont devenues des cibles prisées des pirates du net. Ainsi, une collectivité locale sur 10 déclare avoir été victime d'une de plusieurs cyberattaques au cours des 12 derniers mois selon une étude réalisée par Cybermalveillance.gouv.fr.

Les communes pourront bénéficier d'un soutien financier pour la mise en place de leur plan de sécurisation avec une prise en charge de 50% du coût du projet dans la limite d'un plafond de 200 000€ grâce au « Fonds Innover dans la Ville » de la Métropole du Grand Paris.

Source : https://www.metropolegrandparis.fr/fr/actualites/la-metropole-du-grand-paris-renforce-la-cybersecurite-de-ses-communes-avec-cybiah

Safidy Rasolonjatovo

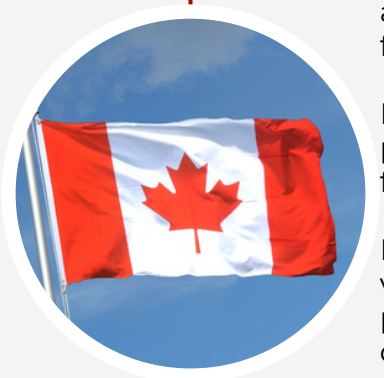
LE GOUVERNEMENT JAPONAIS APPROUVE UN PROJET DE LOI CONTRE LES CYBERATTAQUES

[7 FEVRIER 2025] - Le projet de loi visant à mettre en œuvre ce que l'on appelle la « cyberdéfense active » a été approuvé lors d'une réunion du cabinet ce vendredi 7 février. La législation permettrait à la police et aux forces d'autodéfense japonaises de pirater des sources potentielles de cyberattaques et de les neutraliser avant qu'elles ne puissent mener des attaques.

Le gouvernement conclura des accords avec les opérateurs d'infrastructures critiques, tels que les compagnies d'électricité et de chemin de fer, afin d'avoir accès à leurs communications et de détecter d'éventuelles cyberattaques. Le projet de loi prévoit également la création d'un nouveau poste de vice-ministre chargé de la cybersécurité au sein du secrétariat du cabinet.

Source : https://www3.nhk.or.jp/nhkworld/fr/news/20250207_16/

LE CANADA INVESTIT PRÈS DE 38 MILLIONS DE DOLLARS DANS UNE GRANDE REFONTE DE LA CYBERSÉCURITÉ.



[7 FEVRIER 2025] - Le gouvernement canadien annonce le lancement d'une nouvelle Stratégie nationale de cybersécurité (SNCS) qui proposera une approche innovante pour protéger les citoyens canadiens et les entreprises face aux menaces numériques.

Intitulée « Sécuriser l'avenir numérique du Canada », la SNCS favorisera des partenariats élargis impliquant toutes les sphères de gouvernement, les forces de l'ordre, l'industrie, le monde académique, ect.

De plus, la SNCS donnera à l'État la possibilité de financer des initiatives visant à améliorer la cybersécurité au Canada. Ces initiatives incluront des programmes de sensibilisation et d'éducation. La SNCS est accompagnée d'un investissement initial de 37,8 millions de dollars répartis sur six ans.

Source : https://lesnews.ca/tech/cybersecurite/le-canada-investit-pres-de-38-millions-de-dollars-dans-une-grande-refonte-de-la-cybersecurite/

THERMOMIX : UNE FUITE DE DONNÉES FRAPPE DES UTILISATEURS DU ROBOT DE CUISINE

[7 FEVRIER 2025] - Certains des utilisateurs du robot multifonction Thermomix ont été victimes d'une fuite de données personnelles. Selon l'entreprise Vorwerk, qui commercialise l'accessoire, les informations de certains détenteurs ont été exfiltrées à cause d'une faille de sécurité.

Dans un mail adressé à ses clients, la société explique avoir constaté un « récent incident de sécurité » qui concerne uniquement le forum en ligne. La plateforme permet aux détenteurs d'un robot de cuisine multifonction Thermomix de partager des recettes culinaires entre eux.

Face à cet incident, la firme allemande assure avoir « pris toutes les mesures nécessaires » pour résoudre le problème et qu'aucun mot de passe ou informations financière "sensible" n'a été affecté.

Source : https://www.01net.com/actualites/fuite-donnees-frappe-certains-utilisateurs-robot-thermomix.html

Safidy Rasolonjatovo

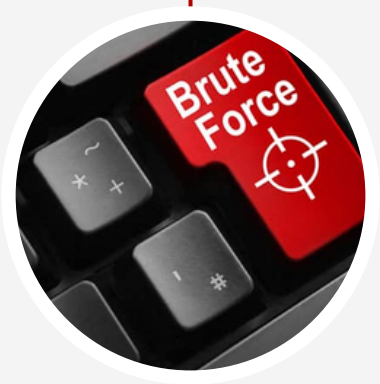
« Passe Ton Hack d'Abord » : le plus grand challenge cyber de France

[7 FEVRIER 2025] - Du 20 janvier au 7 février 2025 se déroule le challenge cyber « Passe Ton Hack d'Abord » dans les lycées de France. Pendant trois semaines, les lycéens de la seconde à la terminale ainsi que les étudiants de BTS et de classes préparatoires sont confrontés au plus grand challenge cyber de France pour les initier aux techniques employées par les cybercombattants.

Pour cette troisième édition, ils sont plus de 7 000 élèves et étudiants à vouloir passer leur « hack » en équipe de 2 à 6 personnes. Ensemble, ils doivent réaliser une quinzaine de challenges autour de la cybersécurité.

Source : https://www.defense.gouv.fr/comcyber/actualites/passe-ton-hack-dabord-2e-edition-elargie-lensemble-du-territoire-francais

UNE ATTAQUE MASSIVE UTILISE 2,8 MILLIONS D'ADRESSE IP POUR PIRATER DES DISPOSITIFS VPN



[10 FEVRIER 2025] - Cette attaque par force brute des mots de passe utilise près de 2,8 millions d'adresses IP pour obtenir les identifiants de connexion de divers appareils VPN.
Il s'agit notamment d'appareils de Palo Alto Networks, Ivanti et SonicWall.

La plupart des adresses IP (1,1 million) proviennent du Brésil, de la Turquie, de la Russie, de l'Argentine, du Maroc et du Mexique. Les cibles des pirates sont les « dispositifs de sécurité périphérique », tels que les pare-feu (VPN).

Les appareils compromis sont majoritairement des routeurs et des objets connectés (IoT) de marque comme Huawei ou Cisco.

Source : https://itdaily.fr/nouvelles/securite/attaque-utilise-2-millions-addresses-ip-pour-pirater-des-vpn/