22 avril 2025 - EDITION N°21

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

CYBERATTAQUE NATIONALE : UN EXERCICE DE CRISE OUVERT À TOUS POUR RENFORCER RÉSILIENCE COLLECTIVE

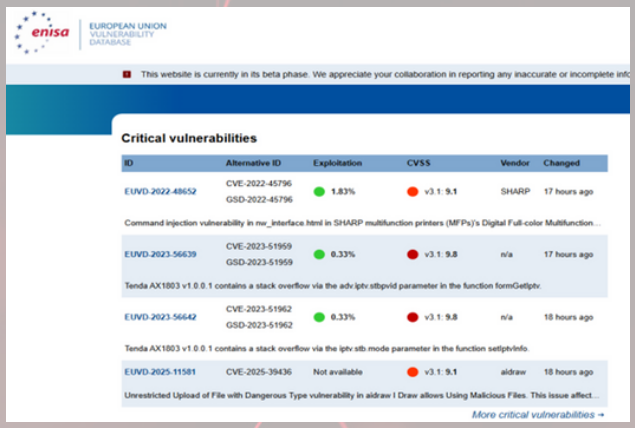
Du 20 avril 2025

Depuis mars 2025, toutes les organisations du pays – entreprises, associations et institutions – sont invitées à participer à REMPAR25, un exercice grandeur nature simulant une cyberattaque d'envergure.
Avec la dépendance croissante aux services numériques, la préparation face aux menaces cyber est devenue une priorité nationale. Le gouvernement français, par l'intermédiaire du COMCYBER, déploie ainsi des stratégies de cyberdéfense ciblant en particulier les secteurs critiques tels que l'eau, l'énergie et les transports.
Sous la supervision de l'ANSSI, plus de 15 000 organisations en France sont désormais soumises à des normes de cybersécurité renforcées.
L'exercice national REMPAR25, prévu pour le 18 septembre 2025, mettra à l'épreuve la résilience des systèmes de sécurité en simulant une crise cyber majeure. L'objectif est de tester non seulement les capacités techniques des équipes de cybersécurité, mais également la coordination avec d'autres services clés comme les ressources humaines, les départements juridiques ou encore la communication.

Source : https://www.radiofrance.fr/franceinfo/podcasts/nouveau-monde/cyberattaque-nationale-un-exercice-de-crise-ouvert-a-tous-pour-renforcer-la-resilience-collective-6937596

https://cyber.gouv.fr/actualites/rempar25-les-inscriptions-sont-ouvertes

FAUTE DE FINANCEMENT LE PROGRAMME CVE DE MITRE EST MENACÉ



Du 16 avril 2025

Le 16 avril dernier, suite à la menace d'un arrêt du financement du programme CVE de MITRE par l'administration américaine, une prolongation temporaire de 11 mois a été accordée grâce à l'intervention du Département de la Sécurité intérieure. D'après certains experts cet arrêt fait partie d'une campagne de réduction des coûts menée par l'administration Trump.
Pour réduire sa dépendance au financement américain, la CVE Foundation a été créée pour poursuivre l'identification et la gestion des vulnérabilités de manière autonome. L'Europe a également réagi, notamment par le biais de l'Enisa, qui a lancé l'European Union Vulnerability Database (EUVD), soutenue par l'UE et le CERT Luxembourgeois. Ce projet vise à assurer une infrastructure européenne solide pour la gestion des vulnérabilités.
Des experts ont souligné que la perte potentielle du CVE créerait de grands défis pour la cybersécurité. En effet, elle pourrait rendre les défenses et les réactions aux menaces moins efficaces. Pour l'avenir, il est recommandé aux organisations de diversifier leurs sources de renseignements sur les menaces et de collaborer avec des partenaires pour pallier toute défaillance du programme CVE.

Source :https://www.forbes.com/sites/kateoflahertyuk/2025/04/16/cve-program-funding-cut-what-it-means-and-what-to-do-next/

LE GROUPE APT 29 DÉPLOIE UN MALWARE CIBLANT DES DIPLOMATES

Du 17 avril 2025

Le groupe APT29, affilié au renseignement russe, a mené une campagne de phishing ciblée contre des ambassades européennes. Dans leur dernière attaque, APT 29 a utilisé une fausse invitation à une dégustation de vin comme appât et diffusé un malware appelé Grapeloader.

Le processus d'infection commence lorsque la victime télécharge et exécute l'archive. Cette dernière utilise du chargement latéral de DLL pour injecter du code malveillant. Grapeloader s'assure de sa persistance sur le système, collecte des informations telles que le nom d'utilisateur et les processus actifs. Puis ces informations sont envoyées à un serveur de commande.Ces informations peuvent servir à des campagnes de déstabilisation ou à connaitre des stratégies commerciales à l'avance. Cette campagne est également marquée par l'utilisation d'une variante de Wineloader, outil précédemment employé par APT29, exploitant la même technique pour contourner les systèmes de détection en utilisant des logiciels légitimes.
En 2023, le groupe avait ciblé des ambassades en Italie, en Roumanie et en Grèce.

Source:https://www.lemondeinformatique.fr/actualites/lire-apt29-deploie-un-malware-ciblant-des-diplomates-96639.html

LA SOCIÉTÉ DE PAIEMENT EN LIGNE ADYEN TOUCHÉE PAR DES CYBERATTAQUES

Du 21 avril 2025

Le fournisseur néerlandais de services de paiement Adyen a subi trois cyberattaques en l'espace de cinq heures lundi soir, entraînant des perturbations dans les magasins, les bars, les restaurants ainsi que dans le commerce de détail en ligne. Ces attaques étaient de type DDoS, visant à paralyser les serveurs en les submergeant de demandes simultanées.

Adyen est l'un des plus grands fournisseurs dans le monde de systèmes de paiement sécurisés. L'entreprise compte parmi ses clients des géants comme Meta, eBay et Uber. L'année dernière, l'entreprise a traité des transactions d'une valeur totale de 1 286 milliards d'euros.

Les attaques ont affecté les services de paiement d'Adyen dans l'Union Européenne, occasionnant des erreurs et des retards de paiement. Les problèmes ont été résolus mardi à 3h30 du matin.

Source : https://www.dutchnews.nl/2025/04/online-payments-firm-adyen-hit-by-easter-monday-cyberattacks/

LES PAYS RENFORCENT LEURS DÉFENSES NUMÉRIQUES DEVANT LA MENACE D'UNE CYBERGUERRE

Du 22 avril 2025

Au printemps dernier, des hackers liés au gouvernement russe ont attaqué des usines de traitement des eaux au Texas, révélant ainsi les vulnérabilités des infrastructures américaines. Cette attaque visait à tester ces infrastructures sans demander de rançon.
Cet événement s'inscrit dans un contexte de tensions géopolitiques croissantes dans lequel les cyberattaques peuvent causer des dommages économiques, perturber des systèmes vitaux et même dégénérer en conflits militaires.
Depuis le début de la présidence de Donald Trump, des réductions de budget et de personnel ont touché les agences de cybersécurité, malgré des appels à renforcer les défenses en matière de cybersécurité. Trump a également limogé des hauts responsables de la NSA et réduit des initiatives de cybersécurité électorale. Pour compenser ces pertes, il a encouragé l'utilisation de l'intelligence artificielle pour améliorer la cyberdéfense.
De experts comme Tom Kellermann appellent à une stratégie plus agressive pour obliger les adversaires à jouer sur la défensive. De plus, la coopération croissante entre des pays comme la Chine, la Russie, l'Iran et la Corée du Nord dans le domaine cyber inquiète les États-Unis. La Chine a été accusée de campagnes de cyberespionnage, bien qu'elle nie ces allégations.

Source : https://lactualite.com/actualites/les-pays-renforcent-leurs-defenses-numeriques-devant-la-menace-dune-cyberguerre/

LE FORUM 4CHAN HORS LIGNE APRÈS UN POSSIBLE PIRATAGE

Du 15 avril 2025

Le forum anonyme 4chan est resté inaccessible pendant plusieurs heures le 15 avril 2025. La panne viendrait d'un piratage qui aurait exposé des données confidentielles. Des messages revendiquant le hack ont été publiés sur le site, accompagnés d'injures racistes et ont impliqué un forum concurrent, Soyjack.
Des documents internes prétendument piratés, incluant des adresses e-mail et des discussions de modérateurs de 4chan, ont été diffusés sur d'autres forums concurrents. Bien que l'authenticité de ces documents n'ait pas été confirmée, leur publication démontre les manquements quant à la sécurité du site. Le forum, sous la propriété d'Hiroyuki Nishimura depuis 2015, est connu pour ses contenus controversés et a déjà été impliqué dans plusieurs affaires judiciaires liées à du cyberharcèlement et à la diffusion de contenus illicites.

Source:https://www.lemonde.fr/pixels/article/2025/04/15/le-forum-4chan-hors-ligne-apres-un-possible-piratage_6596324_4408996.html

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Comment peut-on efficacement contrer les APT sans compromettre les libertés individuelles ?

DONNE TON AVIS DANS LES COMMENTAIRES !