



BULLETIN DE VEILLE CYBER

17 décembre 2024

EDITION N°5



AMAZON ÉCARTE MICROSOFT 365 POUR PROTÉGER SES DONNÉES SENSIBLES

[16 DECEMBRE 2024] - Certains experts critiquent Microsoft pour ne pas avoir assez sécurisé le produit Microsoft 365, malgré les menaces croissantes. Amazon, à son tour décrie un manque de capacités de journalisation et de télémétrie.

La position d'Amazon, en tant que géant technologique, force Microsoft à réagir et à potentiellement renforcer ses outils pour tous les utilisateurs. En revanche, cette décision serait motivée par des intérêts commerciaux, visant à mettre en avant Amazon Web Services (AWS) en tant que solution supérieure.

Source : <https://www.csoonline.com/article/3625205/amazon-refuses-microsoft-365-deployment-because-of-lax-cybersecurity.html>

L'EUROPE RENFORCE SON AUTONOMIE SPATIALE AVEC IRIS² POUR RIVALISER AVEC SPACEX

[16 DECEMBRE 2024] - La Commission européenne a officialisé le projet IRIS², une constellation de 290 satellites prévue pour 2030, afin de garantir la connectivité sécurisée du continent et l'autonomie stratégique de l'Europe dans le secteur spatial.

L'Objectif stratégique affiché est de réduire la dépendance vis-à-vis des acteurs étrangers comme SpaceX (Starlink) pour offrir :

- Une connectivité haut débit pour les citoyens, les entreprises ;
- Un canal sécurisé pour les institutions gouvernementales européennes.

Acteurs clés : SES SA, Eutelsat et Hispasat, Thales Alenia Space, Airbus Defence and Space, Orange et Deutsche Telekom.

Source : <https://www.clubic.com/actualite-547415-l-europe-s-affranchit-de-la-dependance-spatiale-et-concurrence-spacex-avec-son-mega-projet-de-290-satellites.html>

LA NAVIGATION INTERNET DES EMPLOYÉS, UNE FAILLE CRITIQUE EN CYBERSÉCURITÉ

[13 DECEMBRE 2024] - La transformation des environnements de travail, notamment avec l'essor du travail hybride et l'utilisation d'appareils personnels, a bouleversé les paradigmes de la cybersécurité. Une étude de CyberArk, menée auprès de 14 003 employés, révèle que les actions intentionnelles ou accidentelles des collaborateurs augmentent les risques pour les entreprises.

L'étude souligne que les comportements des employés, combinés à des accès à privilèges mal sécurisés, constituent un angle mort majeur de la cybersécurité. Les équipes de sécurité doivent repenser leurs stratégies pour s'adapter aux nouvelles réalités du travail hybride et aux risques croissants liés à l'IA et aux usages personnels des technologies professionnelles.

Source : <https://itsocial.fr/metiers/metiers-articles/la-navigation-sur-internet-dun-employe-langle-mort-de-la-cybersecurite/>



ORANGE SANCTIONNÉ PAR LA CNIL

[12 DECEMBRE 2024] - La CNIL a infligé une amende de 50 millions d'euros à Orange pour :

- Des publicités intrusives dans sa messagerie Mail Orange ;
- Une gestion défectueuse des cookies nonobstant le retrait du consentement par l'utilisateur, ce qui est contraire aux règles du RGPD

Cette décision rappelle la responsabilité des fournisseurs de services numériques en matière de consentement utilisateur et de gestion des cookies. Elle marque une nouvelle étape dans la protection des données personnelles face aux pratiques publicitaires intrusives.

Source : <https://www.solutions-numeriques.com/la-cnil-met-orange-a-lamende/>

RUNET : LA RUSSIE TESTE SA COUPURE DE L'INTERNET MONDIAL POUR RENFORCER SON CONTRÔLE NUMÉRIQUE

[12 DECEMBRE 2024] - La Russie a mené un test grandeur nature de son Internet souverain, Runet, en déconnectant plusieurs régions du pays de l'Internet mondial pendant 24 heures, rendant les VPN inefficaces pour contourner les restrictions.

L'objectif de ce test, piloté par l'autorité des communications Roskomnadzor, est double :

- Assurer l'indépendance numérique en cas de conflit ou de sanctions internationales.
- Renforcer la censure et le contrôle sur l'accès à l'information pour les citoyens russes.

Source : <https://securite.developpez.com/actu/365709/La-Russie-teste-sa-deconnexion-de-l-Internet-mondial-elle-deconnecte-plusieurs-regions-de-l-Internet-mondial-pour-tester-son-Internet-souverain-et-les-VPN-n-ont-pas-aide-les-citoyens-a-contourner-le-blocage/>

CYBERSÉCURITÉ – LES ENTREPRISES VULNÉRABLES DURANT LES FÊTES DE FIN D'ANNÉE

[11 DECEMBRE 2024] - Les experts d'Exponens alertent sur la recrudescence des cyberattaques durant la période de Noël et du Nouvel An, période durant laquelle 75 % des attaques annuelles se produisent. Les entreprises, souvent en effectif réduit et moins vigilantes, sont des cibles de choix pour des cybercriminels de plus en plus structurés.

Techniques d'attaques :

- Ransomware (50 %) : Blocage des systèmes et exfiltration des données contre rançon.
- Phishing et fraudes téléphoniques (40 %) : Fausse identité pour infiltrer les systèmes.
- Fraude au président (10 %) : Usage de l'IA pour imiter la voix d'un dirigeant et détourner des fonds.

Source : <https://lavienumerique.com/articles/204526/cybersecurite-75-des-attaques-se-deroulent-durant-la-periode-de-noel-et-du-nouvel-an.html>