MALIK
DANIAL
BTS2 2024/2025

SUJET : CYBERSÉCURITÉ COMMENT PROTÉGER SES DONNÉES ?

Alerte 1 du 17/01/2025

Cybersécurité des hôpitaux : l'Europe à un plan, mais pas un kopeck

Ce plan prévoit la création d'un centre de soutien au sein de l'Enisa, et un service de réaction rapide. Le financement de tout cela revient aux Etats membres.

PAR LOUIS ADAM
Publié le 17/01/2025 à 16:17 | Mis à jour le 17/01/2025 à 16:18

1 min

Cet article présente le plan d'action de la Commission européenne pour renforcer la cybersécurité dans les établissements de santé (hôpitaux, cliniques, etc.). Il s'agit de protéger ces structures souvent ciblées par des cyberattaques (ex : ransomware, vol de données patients).

- **Un centre de cybersécurité pour les hôpitaux va être créé au sein de l'ENISA (l'agence européenne de cybersécurité).**
- **Il proposera : outils, alertes, accompagnement, détection de menaces.**
- **Un service de réponse rapide aux cyberattaques est aussi prévu, en lien avec une réserve de cybersécurité européenne.**
- **Ce plan s'inscrit dans le cadre de la "cyber solidarité" européenne.**
- **Problème : aucun financement direct n'est prévu pour les hôpitaux ; ce sont les États membres qui doivent payer.**
- **Exemple cité : le plan français "Care" avec 750 millions € jusqu'en 2027 pour audits et équipements.**

Cet article montre que la cybersécurité devient un enjeu de santé publique. Mais aussi que sans financement, même une bonne stratégie reste fragile.Il illustre bien l'écart entre les décisions politiques et la réalité terrain des structures de santé, souvent mal préparées face aux attaques.

Alerte 2 du 10/12/2024

PayPal prend un chemin inquiétant avec nos données

10 décembre 2024 · 12:08

PayPal aimerait bien utiliser notre historique de transaction pour le vendre à des publicitaires.

PayPal, un service de paiement en ligne populaire, annonce un changement important dans ses conditions d'utilisation pour l'été 2025. La plateforme prévoit de partager des informations sur ses utilisateurs pour personnaliser les recommandations d'achat et améliorer l'expérience d'achat. Concrètement, cela signifie que PayPal utilisera des informations sur vos préférences, vos achats passés, ainsi que des détails comme les tailles et styles que vous aimez, pour recommander des produits et services, en collaboration avec les commerçants.

Cependant, certains États américains, comme la Californie, le Dakota du Nord et le Vermont, ont mis en place des lois pour protéger les utilisateurs contre ce changement. Les utilisateurs de ces États ne seront pas affectés. Pour les autres, il sera possible de désactiver cette fonctionnalité en se rendant dans les paramètres de leur compte PayPal, sous la section « Données et confidentialité » puis « expérience d'achat ».

À l'heure actuelle, ces changements ne semblent pas concerner les utilisateurs européens, notamment en France. La version française de PayPal ne propose pas encore cette mise à jour, ce qui pourrait être dû aux réglementations européennes strictes, comme le RGPD et le DMA, qui encadrent la collecte de données personnelles.

Source :
https://www.frandroid.com/culture-tech/web/2435904_paypal-prend-un-chemin-inquietant-avec-nos-donnees

Alerte 3 du 06/12/2024

Victime de phishing sur Signal, le ministre Jean-Noël Barrot refuse de collaborer avec l'Anssi

25 Cybersécurité by Yoann Bourgin / Dec 6, 2024 at 4:06 PM // keep unread // hide

Feedly AI found **2 Companies**

View All

Upgrade to **Feedly Threat Intelligence** to automatically tag CVEs, Threat Actors, Malware Families, TTPs, and IoCs referenced in this article using AI

Learn More

Jean-Noël Barrot, ministre démissionnaire de l'Europe et des Affaires étrangères, a été victime d'une attaque de phishing fin novembre 2024. L'attaque a eu lieu lors d'une réunion du G7, où il a reçu un message via l'application de messagerie sécurisée Signal. Le message contenait un lien malveillant, que Barrot a cliqué sans vérifier la provenance. Ce lien a permis à des cybercriminels d'accéder à son téléphone.

Quelques heures plus tard, le ministre des Affaires étrangères du Bahreïn a reçu un message étrange prétendument envoyé par Barrot, ce qui a alerté ce dernier. L'Anssi (Agence nationale de la sécurité des systèmes d'information) a été rapidement impliquée pour enquêter sur l'incident. L'Anssi a demandé à analyser les données du smartphone de Barrot, mais celui-ci a refusé, invoquant un manque de temps et des déplacements internationaux à venir. Cette décision a retardé l'enquête.

Ce cas soulève plusieurs interrogations. Tout d'abord, Barrot a utilisé son téléphone personnel pour des affaires sensibles, au lieu d'un appareil plus sécurisé. De plus, en

tant qu'ex-ministre chargé du Numérique, Barrot avait porté un projet de loi visant à renforcer la cybersécurité et à lutter contre les attaques de phishing. Ce manque de réactivité et de précaution de sa part a été critiqué, d'autant plus que la situation concerne un ancien responsable de la sécurité numérique.

Source :
https://www.usine-digitale.fr/article/victime-de-phishing-sur-signal-le-ministre-jean-noel-barrot-refuse-de-collaborer-avec-l-anssi.N2223805

Alerte 4 du 05/12/2024

Cyberattaque contre les clients de 8 banques françaises : un virus cherche à piller votre compte

5 décembre 2024 à 11:11

Un malware Android, appelé DroidBot, menace depuis juin 2024 les utilisateurs de smartphones, en particulier ceux de huit banques françaises. Ce virus sophistiqué vole les identifiants bancaires et les mots de passe pour siphonner l'argent des comptes. DroidBot est proposé par des cybercriminels turcs sous forme d'un abonnement Malware-as-a-Service (MaaS) à 3 000 dollars par mois. Plusieurs gangs ont utilisé ce malware pour mener des attaques, notamment dans des pays comme la France, le Royaume-Uni, l'Allemagne et l'Italie.

Les banques françaises concernées sont :

Boursorama
BNP Paribas
Crédit Agricole
Axa Banque
Caisse d'Épargne
Banque Populaire
ING
Société Générale
DroidBot se fait passer pour des applications légitimes comme Google Chrome ou Android Security, pour inciter les utilisateurs à installer le malware. Une fois installé, il enregistre les frappes au clavier, intercepte les SMS (codes de connexion) et peut afficher des fenêtres factices au-dessus des applications bancaires pour voler les données sensibles. Il exploite également les services d'accessibilité Android pour contrôler à distance les appareils infectés.

Les cybercriminels utilisent un panneau d'administration pour personnaliser les attaques, cibler des applications spécifiques et ajuster les attaques en fonction de la langue et des régions. Les chercheurs de Cleafy signalent que DroidBot continue d'évoluer, et de nouvelles fonctionnalités pourraient apparaître.

Les utilisateurs sont invités à éviter d'installer des applications en dehors du Google Play Store, où DroidBot n'a pas encore réussi à se propager.

source:
https://www.01net.com/actualites/cyberattaque-cours-contre-8-banques-francaises-un-virus-cherche-piller-compte.html

Alerte 5 du 27/11/2024

Starbucks perturbé par une attaque ransomware sur un fournisseur tiers

Prasanth Aby Thomas, IDG NS (adapté par Jacques Cheminat) , publié le 28 Novembre 2024

Blue Yonder, éditeur de logiciel de supply chain, a subi une attaque par ransomware. Elle a touché ses clients dont la chaîne de café Starbucks.

Blue Yonder, un éditeur de logiciels spécialisé dans la supply chain, a récemment été victime d'une attaque par ransomware qui a perturbé les opérations de plusieurs de ses clients, dont la célèbre chaîne de café Starbucks. Cette attaque a affecté un système essentiel utilisé par Starbucks pour gérer les horaires et les salaires de ses employés. Cependant, le service à la clientèle de Starbucks n'a pas été impacté.

L'incident a eu lieu dans l'environnement cloud de Blue Yonder, et l'éditeur a immédiatement pris des mesures pour restaurer ses services en collaboration avec des experts en cybersécurité. L'entreprise a travaillé avec Crowdstrike pour rétablir ses systèmes, tout en mettant en place des protocoles de sécurité et de forensique.

Cet incident soulève une problématique importante pour les entreprises : la gestion des fournisseurs et de la chaîne d'approvisionnement en matière de cybersécurité. Les attaques visant les fournisseurs, comme celle subie par Blue Yonder, deviennent

de plus en plus fréquentes, car elles permettent aux pirates de cibler plusieurs entreprises à la fois. Des experts en cybersécurité recommandent de surveiller en continu les fournisseurs, d'évaluer régulièrement leurs mesures de sécurité et d'intégrer des protocoles de résilience dans le plan de continuité des activités des entreprises. Ils suggèrent également de réaliser des revues de code et des tests d'intrusion pour identifier les vulnérabilités critiques.

Source :
https://www.lemondeinformatique.fr/actualites/lire-cyberattaques-des-rancons-toujours-payees-plus-de-donnees-detruites-95474.html

Alerte 6 du 24/10/2024

Chine : les vulnérabilités comme ressource stratégique

Cybersécurité – INTRINSEC par l'Équipe CTI/ 24 octobre 2024 à 10h13

AI Passez à **Feedly Threat Intelligence** pour étiqueter automatiquement les CVE, les acteurs de la menace, les familles de logiciels malveillants, les TTP et les IoC référencés dans cet article à l'aide de l'IA

Apprendre encore plus

L'article parle d'une loi chinoise appelée RMSV qui impose aux entreprises de déclarer rapidement les failles de sécurité, et interdit de les rendre publiques sans accord du gouvernement.

- **Le RMSV est une extension de la loi sur la cybersécurité de 2017.**
- **Obligation de déclarer les vulnérabilités dans les 48h.**
- **Interdiction de rendre publiques les failles sans autorisation.**
- **Conservation des logs pendant 6 mois.**
- **Encouragement des bug bounty internes.**
- **Contrôle étatique sur les chercheurs et les données.**
- **Exploitation potentielle des failles par l'État.**

Cette loi montre une approche très centralisée de la cybersécurité, basée sur la sécurité nationale. Contrairement à l'Europe qui mise sur la transparence, la Chine contrôle fortement les informations. C'est un bon exemple de l'impact des lois sur la cybersécurité.

OUTILS UTILISÉS : FEEDLY, GOOGLE ALERTE