NEWSLETTER SSI SESAN

Bonjour à toutes et à tous,

Quel est le lien entre Cahors, Corbeil-Essonnes et Charleville-Mézières ? La réponse pourrait être que ce sont 3 villes françaises commençant par la lettre C. Eh bien non, c'est un autre point commun qui les relie : ***leurs hôpitaux ont été victimes dernièrement d'une cyberattaque*** *(tiens, encore un C). Les hackers nous enverraient-ils un message ? Dans le doute, si le nom de la ville où se trouve votre structure commence par un « C », soyez cybervigilants ! Plus sérieusement, ces attaques rappellent qu'il ne faut plus attendre avant de mettre des mesures de sécurité, à* ***commencer par des mesures peu onéreuses*** *comme une revue des comptes à privilèges dans l'annuaire d'entreprise et une vérification de ses sauvegardes (déconnectées du réseau).*

En ce ***Cybermois d'octobre****, n'hésitez pas à user et abuser des excellents supports de l'ANSSI(*) pour sensibiliser les utilisateurs !*

Un doute ? Une question ? Contactez-nous sur ssi@sesan.fr !

(*) https://www.ssi.gouv.fr/agence/cybersecurite/le-cybermois/cybermois-2022-tous-ensemble-face-aux-rancongiciels-et-au-hameconnage/

Retour sur les principales attaques >>Lire l'article

Plus de 2 millions d'euros : c'est le coût auquel s'élèverait la réorganisation du fonctionnement du Centre hospitalier Sud francilien (CHSF), à Corbeil-Essonnes (Essonne), à la suite de la cyberattaque par ransomware (rançongiciel) identifiée le 21 août 2022, impactant tout le réseau informatique de l'établissement. Les pirates réclament une rançon de 10 millions de dollars : le CH a tout de suite affirmé qu'il ne paierait pas la somme réclamée.

HEALTH AND TECH, 02/09/2022

L'hôpital de Cahors victime d'une attaque informatique >>Lire l'article

Un établissement de santé supplémentaire est victime d'une cyberattaque ! Cette fois-ci, il s'agit de l'hôpital de Cahors, dans le Lot.

IT-CONNECT, 20/09/2022

Etat des lieux de la menace cyber par le FSSI des ministères sociaux >>Lire l'article

Dans le cadre du congrès de l'Association pour la sécurité des systèmes d'information de santé (Apssis), le fonctionnaire de sécurité des systèmes d'information (FSSI) des ministères sociaux, Jean-François Parguet, a fait récemment un état des lieux de la menace cyber dans le secteur de la santé pour la période 2021/2022.

CYBERVEILLE SANTE, 29/09/2022

Budget 2023 : une enveloppe pour la cybersécurité >>Lire l'article

Le gouvernement a dévoilé, lundi 26 septembre, son projet de loi de finances (PLF) pour 2023. Une part sera attribuée à la lutte contre la cybercriminalité.

L'INFORMATICIEN, 29/09/2022

La nécessité pour les établissements de santé de concilier transformation digitale et cybersécurité *>>Lire l'article*

Pour éviter que ces systèmes deviennent le terrain de jeu des hackeurs, il est nécessaire d'augmenter leur niveau de protection. Pour une sécurisation optimale, il faut :

- Améliorer l'interopérabilité entre toutes les applications utilisées au quotidien par les établissements de santé.
- Mettre en place et encadrer le développement des télé activités avec des applications sécurisées.
- Intégrer une solution de sécurisation de messageries, l'email représentant le vecteur principal d'attaque.

DSIH, 30/09/2022

BONNES PRATIQUES

Que faire en cas de piratage de compte sur les réseaux sociaux ? *>>Lire l'article*

Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter, WhatsApp… Vous avez remarqué une activité suspecte ?

CYBERMALVEILLANCE.GOUV, 02/09/2022

Perte ou vol de matériel informatique nomade : les bons réflexes à avoir *>>Lire l'article*

Régulièrement, la CNIL communique sur des violations de données typiques inspirées d'incidents réels qui lui sont notifiés. La présente publication a pour objectif d'expliquer comment se protéger lors de l'utilisation de supports amovibles pouvant contenir des données personnelles.

CNIL, 15/09/2022

CYBERMOI/S 2022 : Agir ensemble face aux rancongiciels *>>Lire l'article*

Pendant tout le mois d'octobre, le Cybermoi/s partage des astuces simples pour vous aider à vous prémunir contre les cyber attaques.

ANSSI, 22/09/2022

MENACES

Bond de 75 % des attaques ransomware sur les systèmes Linux au S1 2022 *>>Lire l'article*

Une étude menée par Trend Micro avec Sapio Research auprès de 6 297 responsables en sécurité informatique de 29 pays montre une augmentation de 75% sur un an du nombre d'attaques par ransomware ciblant les systèmes Linux au cours du premier semestre 2022. Les variantes des ransomwares LockBit et Cheerscrypt pour environnements Linux virtualisés sous VMware ESXi sont toujours aussi virulentes.

LMI, 06/09/2022

Les cybercriminels multiplient les attaques ciblant des protocoles industriels *>>Lire l'article*

Selon le dernier rapport de Nozomi Networks Labs, les wipers et les botnets IoT dominent le paysage des menaces. Les secteurs de la fabrication et de l'énergie sont les plus menacés.

IT SOCIAL, 12/09/2022

SMB, SSH, Telnet…Les protocoles oubliés de la cyber sécurité *>>Lire l'article*

L'analyse des environnements informatiques fait ressortir un pourcentage important d'organisations qui exposent des protocoles non sécurisés ou sensibles sur Internet, dont SSH est le plus exposé.

IT SOCIAL, 30/08/2022

Multiples vulnérabilités dans Baxter *>>Lire l'article*

Les multiples vulnérabilités dans Baxter Spectrum WBM peuvent permettre à un attaquant de de modifier des paramètres et d'empêcher la connexion au réseau, de lire dans la mémoire WBM, d'extraire des informations sensibles ou de provoquer un déni de service.

CYBERVEILLE SANTE, 12/09/2022

Multiples vulnérabilités dans Microsoft Exchange *>>Lire l'article*

En date du 29 septembre 2022, Microsoft a indiqué l'existence de deux vulnérabilités, de type zéro-jour, au sein de Windows Exchange 2013, 2016 et 2019. Ces vulnérabilités sont les suivantes :

- CVE-2022-41040 : Vulnérabilité de type injection de requêtes forgées côté serveur (Server Side Request Forgery, SSRF) exploitable par un attaquant authentifié ;
- CVE-2022-41082 : Vulnérabilité permettant à un attaquant authentifié d'exécuter du code arbitraire à distance.

CERT-FR, 30/09/2022

RGPD/ JURIDIQUE

Diffusion de données piratées à la suite d'une cyberattaque : quels sont les risques et les précautions à prendre ?.

>>Lire l'article

La CNIL constate une nette progression des notifications de violation de données dont près de la moitié résultent d'une attaque par rançongiciel. Dans certains cas, les données personnelles des usagers peuvent être mises en ligne par les pirates. La CNIL répond aux questions des personnes potentiellement concernées.

CNIL, 26/09/2022

Entrepôts de données de santé : la CNIL publie une « check-list » de conformité à son référentiel

>>Lire l'article

La création d'un entrepôt de données de santé nécessite le respect de certaines formalités. Afin de simplifier les démarches pour les responsables de ces bases de données sensibles, la CNIL a adopté en octobre 2021 un référentiel. En complément, elle propose aujourd'hui une « check-list » de conformité.

CNIL, 28/09/2022

Les entrepôts de données de santé hospitaliers face au DGA

>>Lire l'article

Alors que les premières candidatures de l'appel à projets « Accompagnement et soutien à la constitution d'entrepôts de données de santé hospitaliers » vont être prochainement relevées, il est plus qu'utile d'interroger la constitution de tels entrepôts à l'aune du règlement européen sur la gouvernance des données (Data Governance Act - DGA) qui entrera en application dans moins d'un an, le 24 septembre 2023.

DSIH, 30/09/2022

TRUCS ET ASTUCES

Conseils pour sécuriser votre réseau de santé

>>Lire l'article

Pour vous protéger des cyberattaques, il est conseillé de commencer avec un plan en trois axes, à savoir la prévention, la détection et la surveillance. Voici quelques recommandations pour chaque axe.

DSIH, 06/09/2022

PODCAST – Professionnalisation des attaquants

>>Lire l'article

Cet épisode traite de l'évolution de l'écosystème des attaquants. De l'amateurisme à l'extrême professionnalisation.

NO LIMIT SECU, 18/09/2022