NEWSLETTER SSI SESAN

Bonjour à toutes et tous,

La fin des congés d'été nous a ramené brutalement à la réalité avec ***la cyberattaque qui a touché le Centre Hospitalier Sud Francilien*** *(CHSF). A l'heure où parait cette Newsletter, la remise en fonction du SI est toujours en cours. Cette attaque n'est malheureusement pas la dernière (d'ailleurs, trois jours plus tard, c'est un EHPAD de l'Eure qui a été touché par un cryptolocker). Pour autant, il ne faut pas baisser les bras et continuer à améliorer la sécurité des SI : les mesures de sécurité ne nous protègent pas de tout incident, mais elles permettent d'en limiter les conséquences.*

Toujours ***dans une démarche d'accompagnement des structures de santé et du médico-social****, nous vous proposerons des actions complémentaires à notre offre de sécurité dans les prochaines semaines.*

Vous souhaitez découvrir nos services et solutions : contactez-nous sur ssi@sesan.fr !

Le coût moyen d'une violation de données a bondi de 13 % depuis 2020 >>Lire l'article

Les violations de données sont plus coûteuses et plus impactantes que jamais, le coût moyen d'une violation de données atteint le chiffre record de 4,35 millions de dollars au niveau mondial en 2022.

IT SOCIAL, 28/07/2022

Le secteur de la santé est une cible particulièrement vulnérable >>Lire l'article

Charlotte Drapeau (ANSSI) : « L'augmentation de la menace cyber reste particulièrement inquiétante puisque 203 attaques par rançongiciels ont été portées à la connaissance de l'ANSSI en 2021, après une multiplication par 4 du nombre d'attaques traitées par l'agence les deux années précédentes, passant de 54 en 2019 à 192 en 2020. »

SANTE ACHAT INFO, 28/07/2022

Les applications mobiles de santé, utiles mais encore trop peu contrôlées >>Lire l'article

Selon une récente étude publiée dans le Journal of Medical Internet Research, 64% des applications de «e-santé» n'auraient pas réalisé d'étude clinique pour démontrer leur efficacité.

LA FIGARO, 15/08/2022

Deux concertations estivales proposées par l'Agence du Numérique en Santé *>>Lire l'article*

L'Agence du numérique en santé continue ses concertations même au cœur de l'été. La première d'entre elles concerne Mon espace Santé ainsi que les spécifications des API d'interopérabilité, et la seconde les volets CI-SIS du projet de diffusion d'imagerie médicale du Ségur du numérique en santé.

DSIH, 16/08/2022

Le gouvernement met 20 millions d'euros sur la table pour les hôpitaux *>>Lire l'article*

Face à la multiplication des cyberattaques contre les hôpitaux, le gouvernement a promis vendredi 26/08 de renforcer les moyens financiers mis à la disposition des établissements de santé pour renforcer leur sécurité informatique.

LES ECHOS, 28/08/2022

BONNES PRATIQUES

5 mesures pour bien gérer les crises de cybersécurité *>>Lire l'article*

La gestion des crises de cybersécurité est essentielle pour prévenir et gérer les conséquences d'une attaque. Il est donc important de préparer une réponse efficace aux crises de cybersécurité en mettant en place des procédures et en formant les équipes. En cas d'attaque, il faut réagir rapidement pour limiter les dégâts et appliquer une stratégie de récupération des services.

LE MONDE INFORMATIQUE, 18/07/2022

APF France handicap mobilise ses collaborateurs contre les cyberattaques *>>Lire l'article*

face aux risques de cyberattaques, l'association APF France handicap a choisi de sensibiliser tous ses collaborateurs afin d'adopter de bonnes pratiques et éviter les pièges. Pour mener à bien cette mission, elle a fait appel à une société spécialisée proposant une solution ad-hoc.

ZDNET, 25/07/2022

Comment réagir en cas d'attaque par rançongiciel ? *>>Lire l'article*

Alerter, isoler les supports, monter une cellule de crise, communiquer… Plusieurs bonnes pratiques peuvent être mobilisées par les établissements de santé ou médico-sociaux en cas d'attaque par rançongiciel.

HOSPIMEDIA, 03/08/2022

MENACES

Augmentation de 94 % des attaques par rançongiciel en 2021 dans le secteur de la Santé [>>Lire l'article]

La firme britannique de cybersécurité Sophos a publié son rapport 2022 concernant l'état de la menace « rançongiciel » dans le monde de la santé. Les données présentées dans celui-ci montrent l'augmentation rapide de ces attaques et l'ampleur des impacts subis par les structures qui en sont victimes.

CYBERVEILLE SANTE, 28/06/2022

Microsoft a découvert une campagne de phishing ayant touché 10 000 entreprises [>>Lire l'article]

La firme de Redmond a publié les détails d'une attaque par hameçonnage capable d'outrepasser les comptes protégés avec une double authentification. Au moins 10 000 entreprises auraient été touchées depuis septembre dernier..

01.NET, 13/07/2022

2022-2023 : données de santé, cible n°1 des escrocs et des black hat [>>Lire l'article]

Les opérations de phishing ciblant les organismes hébergeant des données de santé, ou liées à la santé se multiplient.

FORBES 09/08/2022

Quand le niveau technique monte, les attaquants se recentrent sur les utilisateurs *>>Lire l'article*

Lorsqu'il s'agit d'atteindre leurs objectifs : s'introduire dans les systèmes d'informations de leurs victimes, exfiltrer les données et les chiffrer avant de partir, les acteurs du rançongiciels ne se posent pas vraiment de questions, si techniquement ce n'est pas facile de rentrer, autant demander à un bon samaritain d'ouvrir la porte.

DSIH, 16/08/2022

Un Ehpad à son tour victime d'une cyberattaque dans l'Eure *>>Lire l'article*

Le Groupe hospitalier du Havre, dont relève l'établissement pour personnes âgées, a précisé que des données sensibles avaient été chiffrées, entraînant "un système d'information inaccessible". Heureusement, la prise en charge des patients ne serait pas impactée.

LES NUMERIQUES, 25/08/2022

Les API, maillons faibles de la sécurité du cloud *>>Lire l'article*

Les interfaces de programmation d'applications font désormais partie intégrante de nombreux services cloud. Mais elles sont aussi une cible de choix pour les attaquants, au point de représenter dorénavant une menace majeure.

LE MONDE INFORMATIQUE, 14/07/2022

Vulnérabilités critiques du 22/08/22 au 29/08/22 *>>Lire l'article*

Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine 38 pour souligner leurs criticités.

Toutes les vulnérabilités évoquées dans les avis du CERT-FR doivent être prises en compte et faire l'objet d'un plan d'action lorsqu'elles génèrent des risques sur le système d'information.

CERT-FR, 29/08/2022

RGPD/ JURIDIQUE

Le MOOC de la CNIL est de retour dans une nouvelle version enrichie. >>Lire l'article

L'atelier RGPD est une formation en ligne gratuite, illimitée et ouverte à tous (Mooc). Elle permet de sensibiliser les professionnels à la protection des données et d'accompagner leur mise en conformité. Dans cette nouvelle version, la CNIL propose un nouveau module dédié aux collectivités territoriales.

CNIL, 27/06/2022

Interview Nicolas Bourgeois (AFCDP) >>Lire l'article

Nicolas Bourgeois, membre de l'AFCDP (association française des correspondants à la protection des données à caractère personnel) a participé à la Cybermatinée Sécurité du Monde Informatique, organisée le 19 mai 2022 à Lille. Lors de son intervention, il est notamment revenu sur la nécessité d'intégrer les métiers pour assurer la réussite des projets de mise en conformité RGPD.

LE MONDE INFORMATIQUE, 22/07/2022

Les CNIL européennes adoptent un avis sur l'Espace européen des données de santé >>Lire l'article

Le 12 juillet 2022, le Comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données ont adopté un avis sur l'Espace européen des données de santé et sélectionné trois cas transfrontaliers stratégiques pour lesquels prioriser une coopération renforcée

CNIL, 01/08/2022

TRUCS ET ASTUCES

Comment savoir si un site est fiable ? *>>Lire l'article*

Afin de rester en sécurité lorsque vous naviguez sur la toile, vous devez connaître les bonnes pratiques de la sécurité numérique. Vous saurez ainsi reconnaître si un site est fiable ou non.

BUZZ WEBZINE, 24/07/2022

Remettre en état un système d'information après une cyber-attaque, un marathon ? *>>Lire l'article*

A la lecture de du témoignage du CH de Dax, rendu public par Aline Gilet-Caubère, directrice adjointe de l'hôpital, on constate l'importance cruciale de disposer de sauvegardes protégées afin qu'elles ne soient pas elles aussi abimées ou verrouillées par du cryptage par l'attaque cyber.?

LA REVUE DIGITALE, 28/07/2022

Unprotect Project : comprendre les codes malveillants *>>Lire l'article*

Un outil étonnant et passionnant que le projet Unprotect. Il permet de comprendre les logiciels malveillants pour mieux s'en défendre. Un puit de connaissances sur les pratiques de détection afin de raccourcir les temps de réponse des protecteurs. UP propose un catalogue de plus de 200 astuces utilisées par les malwares qui tentent, par millions chaque jour, de contourner les outils de détection et de protection.

ZATAZ, 18/08/2022