NEWSLETTER SSI SESAN

Bonjour à toutes et tous,

Notre communauté de RSSI Santé franciliens s'accroit avec de nouveaux membres. ***Nous sommes désormais près de 40 adhérents****, regroupant plus de 100 établissements qui bénéficient de nos services et peuvent s'entraider grâce à notre réseau SESAN.*

Une activité dense pour le département Sécurité des Systèmes d'Information de SESAN en juin :

- ***Le 9 juin, notre comité de pilotage SSI*** *a permis de revenir sur notre offre de services et sur ses perspectives d'évolution en 2023. N'hésitez pas à nous remonter vos besoins si vous ne pouviez être présents !*
- ***Le 16 juin, notre webinaire sur le kit d'exercice de cybercrise de l'ANS*** *a réuni plus de 100 personnes. L'occasion de présenter le travail réalisé par le Groupe de Travail Territorial SSI, piloté par l'ANS et auquel SESAN est associé en sponsor (avec les régions Pays-de-Loire, Bourgogne-Franche-Comté et la Réunion).*
- ***Le 23 juin était organisé notre comité de pilotage sur la conformité RGPD****, avec la présentation des webinaires « pratiques » à venir ;*
- ***Le 24 juin, réunion du groupe de travail Opérateurs de Services Essentiels (OSE)****, avec un point d'avancement sur les mesures de sécurité obligatoires un an après la désignation, la fourniture d'un outil de reporting et le nouveau dispositif d'accompagnement de l'ANSSI dans le cadre de France Relance. Le GT OSE se réunira tous les 2 mois (prochain rendez-vous le 2 septembre).*

La Newsletter SSI revient en septembre, mais nous restons mobilisés. Pensez à souscrire à notre service de cybersurveillance 24x7 !

Un sujet vous intéresse*, vous souhaitez découvrir nos services et solutions : contactez-nous sur ssi@sesan.fr !*

Un arrêté va intégrer 5 modules sur le numérique en santé dans le cursus universitaire *>>Lire l'article*

Daté du 23 février 2022, ce référentiel de la DNS a été co-construit par l'ensemble des représentants des formations des professionnels de santé (formation initiale ou en exercice). Il précise les compétences qui feront partie du cursus universitaire, articulées en 5 modules pour un total 28 heures dont 5 heures de cybersécurité.

HEALTH AND TECH, 14/06/2022

Sécurité des Système d'Information Hospitalier (SIH) : la blockchain *>>Lire l'article*

Le secteur de la santé est donc en train d'opérer sa transformation mais reste vulnérable pendant cette phase de transition. Une autre piste est en train d'émerger pour renforcer la sécurité des SIH: la blockchain. elle permettrait d'assurer la sécurité des données de santé et de sécuriser le stockage, de favoriser l'interopérabilité des SI.

HEALTH AND TECH, 17/06/2022

Sécurité des SI de santé : un renforcement nécessaire impulsé par l'Etat *>>Lire l'article*

En 2021, la cybersécurité est devenue une priorité nationale traitée au plus niveau de l'Etat : plans, programmes dédiés, financements, certifications, ...

DSIH, 20/06/2022

BONNES PRATIQUES

Prévenir les cyberattaques et protéger ses données >>Lire l'article

Les professionnels libéraux sont les premiers concernés par les cyberattaques. Un comportement rigoureux permet de s'en prémunir et de protéger les données de leur patient. Vincent Croisile, expert sécurité à l'Agence du Numérique en Santé (ANS) précise toutefois ne pas pouvoir fournir de chiffres concernant les cyberattaques subies par libéraux car ils n'ont pas d'obligation de les déclarer.

ACTU SOINS, 27/05/2022

États-Unis : La Food and Drug Administration (FDA) publie des recommandations de sécurité concernant le matériel médical connecté >>Lire l'article

La multiplication de l'Internet des Objets (IOT) dans la sphère médicale s'accompagne d'une augmentation importante de probabilité de cyber attaques contre des dispositifs médicaux et les réseaux auxquels ceux-ci peuvent être reliés. Pour couvrir ces menaces, la FDA (Food and Drug Administration) a commencé à définir des directives prévoyant le maintien d'un haut degré de sécurité tout au long du cycle de vie des logiciels et produits connectés répondant à une mission de santé..

CYVERVEILLE SANTE, 02/06/2022

Objets médicaux connectés : les défis au-delà de la cybersécurité? >>Lire l'article

Comment fonctionnent les systèmes de l'IoMT ? Quelles sont les 5 enjeux techniques majeures pour optimiser l'utilisation de l'IoMT ?

PROGRAMMEZ, 02/06/2022

MENACES

Belgique : Le groupe d'établissements Vivalia paralysé par un rançongiciel >>Lire l'article

Le 14 mai 2022, le groupement luxembourgeois intercommunal de santé Vivalia a été la cible du groupe rançongiciel Lockbit. Le groupe de santé Vivalia, qui gère sept hôpitaux et six centres de soins résidentiels, fonctionne actuellement en mode dégradé à la suite d'une attaque rançongiciel ayant affecté 200 serveurs et 1500 PC au sein de ses réseaux..

CYBERVEILLE SANTE, 01/06/2022

Costa Rica : Le système de santé de santé hors service >>Lire l'article

L'institution costaricienne précise que le ransomware Hive a été déployé sur au moins 30 des 1 500 serveurs gouvernementaux et qu'il est impossible d'estimer le temps de récupération.

SIECLE DIGITAL, 02/06/2022

1 million de comptes AMELI en vente par un pirate ? >>Lire l'article

Le Service Veille ZATAZ a repéré une vente de données qui laisse présager des cyberattaques de masse, cet été, à destination des assurés sociaux français. Le SVZ a repéré une vente d'un million de comptes.

ZATAZ, 23/06/2022

Vulnérabilités significatives de la semaine 24 *>>Lire l'article*

Le bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine du 13/06/22 au 17/06/22 pour souligner leurs criticités. Il ne remplace pas l'analyse de l'ensemble des avis et alertes publiés par le CERT-FR dans le cadre d'une analyse de risques pour prioriser l'application des correctifs.

CERT-FR, 21/06/2022

Électrocardiographes de repos Welch Allyn : deux vulnérabilités identifiées *>>Lire l'article*

Le 16 juin 2022, Hillrom Medical Device Management a publié deux vulnérabilités affectant des électrocardiographes de repos Welch Allyn.

L'exploitation de ces vulnérabilités, dont les scores CVSS de gravité respectifs s'étendent de « moyen » à « élevé », permettrait à un attaquant non autorisé d'exécuter du code arbitraire avec des paramètres élevés et d'avoir accès à des informations médicales confidentielles.

CYBERVEILLE SANTE, 23/06/2022

RGPD/ JURIDIQUE

Commande publique : quel acteur est responsable au regard du RGPD ?. >>Lire l'article

Afin d'aider les professionnels concernés à identifier leurs responsabilités dans différents contextes de commande publique, la CNIL clarifie les éléments à prendre en compte et les conséquences juridiques à tirer de la qualification de « responsable du traitement », de « sous-traitant » ou « responsable conjoint ».

CNIL, 02/06/2022

La gestion des risques cyber : quelles obligations pour les OIV ? >>Lire l'article

« Dans un contexte où le niveau d'exposition de l'ensemble des acteurs publics comme privés au risque cyber ne cesse d'augmenter, (le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37% en 2021), les Opérateurs d'Importances Vitales (OIV) ont une place à part.

Les OIV sont en effet tenus de mettre en place des mesures de sécurité spécifiques afin de protéger leur Système d'Information d'Importance Vitale. »

HAAS AVOCATS 09/06/2022

RGPD en santé : les enjeux des cinq prochaines années >>Lire l'article

Il reste des sujets en friche, des domaines où le DPO s'interroge sur le mode de résolution, et aussi des difficultés initialement non prévues que pas grand monde n'a vu arriver sur le terrain…

DSIH , 21/06/2022

TRUCS ET ASTUCES

4 Fables détournées pour sensibiliser à la cybersécurité. [>>Lire l'article]

Pour les sensibiliser à la cybersécurité et déconstruire les préjugés des élus et Directions générales des Services, Cybermalveillance.gouv.fr a réalisé une série de quatre films, illustrant les objections sous forme de fables, pour interpeller ces derniers aux conséquences d'une cyberattaque.

Pour prévenir ces risques, chacune des vidéos se conclut par une morale de fable unique.

CYBERMALVEILLANCE.GOUV, 01/06/2022

Google Analytics et transferts de données : comment mettre son outil de mesure d'audience en conformité avec le RGPD ? [>>Lire l'article]

L'utilisation d'un proxy correctement configuré peut, cependant, constituer une solution opérationnelle pour limiter les risques pour les personnes Quelles sont les mesures à mettre en place pour que la « proxyfication » soit valable ?

CNIL, 07/06/2022

Fuite de données : un plan de réponse en 5 étapes [>>Lire l'article]

Si une organisation est victime d'une fuite de données, il faut qu'elle ait un plan pour remédier à la situation, minimiser l'impact et assurer la continuité des activités. Bien qu'il n'existe pas de pratique universelle, les étapes suivantes sont essentielles pour obtenir un résultat positif.

GLOBAL SECURITY MAG, 20/06/2022