n°41
Août 2023

sesan
Groupement d'Intérêt Public eSanté

Newsletter Cybersanté

L'actualité sur la cybersécurité du mois précédent proposée par le GRADeS d'Île-de-France

TOUS CYBER VIGILANTS

Edito

Bonjour,

Le département SSI et les cyberservices continuent de s'enrichir :

- Nous vous proposons pour les semaines à venir des formations (PCA et Sécurité Microsoft 365).

- Plusieurs structures ont manifesté leur volonté de tester le kit PCA/PRA de l'ANS. L'équipe sera présente auprès des structures qui le souhaitent pour observer cette phase pilote et être en capacité de vous accompagner par la suite.

- Nous allons évaluer de nouveaux services (voir les publications sur notre plateforme d'échange).

- Un nouvel appel d'offres est en préparation pour pouvoir enrichir notre assistance sur les actions de remédiation technique (suite à un audit par exemple).

Nous vous donnons rendez-vous prochainement sur tous ces sujets.

Bonne rentrée à toutes et tous.

Un doute ?

Une question ?

Contactez-nous sur
ssi@sesan.fr

Actus à la une

PUBLICATION D'UN OUTIL D'AUTOÉVALUATION DE GESTION DE CRISE CYBER

L'ANSSI propose un outil d'autoévaluation basé sur sa collection de guides de gestion de crise cyber. Cet outil, développé en collaboration avec le CDSE, comprend 57 questions réparties en 5 thèmes et permet aux organisations d'évaluer leur préparation aux crises cyber, offrant des indicateurs et des recommandations pour améliorer leur niveau de maturité et de continuité.. Les organisations sont encouragées à partager leurs résultats avec l'ANSSI pour aider à renforcer la vision du niveau de maturité de l'écosystème français.

Lire l'article

ANSSI, 04/07/2023

CYBERSÉCURITÉ: TOUS LES HÔPITAUX POTENTIELLEMENT CONCERNÉS PAR LA DIRECTIVE NIS 2

Lire l'article

La directive européenne NIS 2 sera intégrée dans le droit français pour la sécurité des systèmes d'information de la santé. Tous les établissements de santé, publics et privés, probablement plus de 250 salariés, seront soumis à des règles de sécurité, différenciées selon leur importance, avec une mise en vigueur d'ici au second semestre 2024, supervisée par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

TIC SANTÉ, 06/07/2023

PLUS DE 500 ÉTABLISSEMENTS DE SANTÉ ONT RÉCEMMENT EFFECTUÉ AU MOINS UN EXERCICE INITIAL DE GESTION DE CRISE CYBER.

Pour contrer les cyberattaques croissantes contre les établissements de santé, des exercices de gestion de crise cyber sont désormais indispensables, avec un objectif gouvernemental de 50% des établissements formés d'ici décembre 2023 via le programme CaRE qui promeut la sécurité opérationnelle et la sensibilisation.

Lire l'article

ANS, 27/07/2023

Bonnes pratiques

CYBERATTAQUES DANS LES HÔPITAUX, UNIVERSITÉS, ADMINISTRATIONS... COMMENT MIEUX RÉSISTER ?

Environ 24,21 % des cybermenaces mondiales depuis juillet 2021 ont ciblé des administrations publiques, avec un risque sous-estimé en France malgré des attaques fréquentes en 2019. Les administrations souffrent de vulnérabilités dues à des ressources limitées et à un recrutement restreint d'experts en cybersécurité, nécessitant une résilience technique et organisationnelle renforcée.

Lire l'article

CONTRE POINTS, 01/07/2023

LE CERT SANTÉ PUBLIE UNE FICHE CONCERNANT L'UTILISATION DES EDR

Lire l'article

L'adoption croissante des EDR dans les établissements de santé a motivé le CERT Santé à créer une fiche de synthèse, mettant en lumière les conditions favorables à l'amélioration de la sécurité des systèmes d'information grâce à cette technologie.

CERT SANTÉ, 03/08/2023

SÉCURITÉ DES SYSTÈMES À RISQUE MAJEUR EN CAS DE VIOLATION : LA CNIL LANCE UNE CONSULTATION PUBLIQUE SUR UN PROJET DE RECOMMANDATION

La CNIL propose une recommandation visant à regrouper les pratiques avancées de sécurité pour les traitements de données personnelles à risques majeurs, en particulier pour les traitements "critiques" définis par des critères de grande échelle et d'impact potentiel important. La consultation publique, ouverte jusqu'au 8 octobre 2023, s'adresse aux responsables de tels traitements et à tout organisme intéressé. La recommandation finale sera publiée début 2024 après prise en compte des retours.

Lire l'article

CNIL, 28/08/2023

Menaces

LES HACKERS EXPLOITENT DE NOUVELLES PRATIQUES D'INGÉNIERIE SOCIALE COMME LES NOTIFICATIONS DES NAVIGATEURS WEB

Les attaquants utilisent des tactiques d'ingénierie sociale via les navigateurs pour le hameçonnage et adoptent des approches "living-off-the-land". Les hackers ont un avantage du fait de leur motivation élevée et peuvent se focaliser sur des vulnérabilités spécifiques, tandis que les défenseurs font face à des systèmes complexes avec des ressources limitées. La menace étatique est en hausse, principalement de la part de la Russie et de la Chine, tandis que les attaques "living-off-the-land", les attaques Linux et les maliciels "zeroday" préoccupent également. Une approche recommandée est l'adoption d'une plateforme de sécurité unifiée.

Lire l'article

IT SOCIAL, 03/07/2023

[UNION EUROPÉENNE] : RAPPORT ENISA DES CYBERMENACES CONCERNANT LE SECTEUR DE LA SANTÉ

Lire l'article

L'Agence européenne pour la cybersécurité (ENISA) a publié un rapport sur les menaces cyber dans le secteur de la santé pour 2021-2022, basé sur 215 incidents en Europe. Les attaques touchent principalement les hôpitaux (42%), impliquent des rançongiciels (54%) et des fuites de données. Les recommandations de l'ENISA incluent des sauvegardes hors ligne, la sensibilisation, la gestion des vulnérabilités, les correctifs logiciels, l'authentification à double facteur, les plans d'intervention et l'engagement des décideurs dans la gestion des risques.

CERT SANTÉ, 20/07/2023

RHYSIDA RANSOMWARE : UN NOUVEAU RISQUE POUR LE SECTEUR DE LA SANTÉ

Le groupe de rançongiciel Rhysida Ransomware, découvert en mai 2023, opère en tant que fournisseur de RaaS. Ciblant principalement l'industrie, l'éducation et la santé, le groupe utilise l'hameçonnage avec Cobalt Strike pour infecter, puis déploie un exécutable Windows Rhysida pour chiffrer les fichiers avec l'algorithme ChaCha20. Le paiement de la rançon en Bitcoin s'effectue via leur site sur le dark web. Le Centre de coordination de la cybersécurité du secteur de la santé américain (HC3) a publié une alerte à ce sujet.

Lire l'article

CERT Santé, 18/08/2023

Juridique

VAL-DE-MARNE : LA PROFESSEURE EN MÉDECINE NUCLÉAIRE SE VENGE EN SUPPRIMANT 4 500 FICHIERS À L'HÔPITAL

Une professeure en médecine nucléaire a été placée en garde à vue à Paris pour avoir supprimé des fichiers stratégiques de l'hôpital du Kremlin-Bicêtre où elle travaillait, en représailles au non-renouvellement de son contrat. Malgré ses dénégations, des preuves la reliant aux faits ont été trouvées, et elle a été remise en liberté en attente de son procès en mars 2024.

Lire l'article

LE PARISIEN, 08/07/2023

LES DROITS D'ACCÈS AU DMP PAR LES PROFESSIONNELS DU MÉDICO-SOCIAL REVUS PAR UN PROJET D'ARRÊTÉ

Lire l'article

Un projet d'arrêté en discussion permettrait l'accès élargi au dossier médical partagé (DMP) pour de nouvelles professions médico-sociales, définissant les règles de gestion des droits d'accès par arrêté ministériel. Une matrice d'habilitation, accompagnant le projet de texte, établit les règles de lecture des contenus du DMP selon les professions habilitées. Les professionnels du médico-social seraient inclus, conformément à la loi de décembre 2020, avec un accès limité aux données nécessaires à leur rôle, tout en maintenant le contrôle des citoyens sur leurs données de santé.

TIC SANTÉ, 18/08/2023

LE BYOD, UNE PRATIQUE UTILE POUR LES ENTREPRISES MAIS À ENCADRER

La tendance BYOD offre des avantages mais présente des risques de sécurité pour les entreprises. Les questions juridiques telles que la confidentialité et la propriété intellectuelle doivent être résolues. Les solutions techniques telles que le cryptage, les VPN et le MDM peuvent contribuer à sécuriser les appareils personnels utilisés au travail.

Lire l'article

LEXING - BENSOUSSAN AVOCATS, 24/08/2023

ILE-DE-FRANCE

sesan

Groupement d'Intérêt Public **eSanté**