

#24 Février 2022

NEWSLETTER SSI SESAN



sesan

Bonjour à tous,

En 2022, le numérique en santé n'a jamais été autant soutenu, il va se développer avec son cortège de patchs de sécurité manquant(1), de défauts de configuration(2) et d'utilisateurs sensibles aux courriels frauduleux(3). **L'année 2022 s'annonce riche en événements cyber**, et il faut s'attendre à de nouveaux incidents dans les semaines et mois à venir. Face à ces menaces, **SESAN met à votre disposition des services de protection** :

1. **Un scanner de vulnérabilité**, sans limite d'adresses IP, que chaque structure peut gérer elle-même ou en étant accompagnée par SESAN : le prochain « log4j » pourra ainsi être traité efficacement ;
2. **Une cybersurveillance permanente** qui détecte les failles et les fuites de données sur le darkweb : plusieurs interfaces d'administration ont ainsi pu être sécurisée avant qu'une malveillance ne survienne ;
3. **Des tests de phishing associés à une sensibilisation contextualisée** : en réalisant des tests plusieurs fois par an, le nombre de clics diminue drastiquement.

Comme les mesures barrières face aux virus, ces mesures réduisent le risque mais ne l'éliminent pas complètement. C'est pourquoi **nous vous avons proposé en 2021 des exercices de cybercrise**(*). Ces exercices seront prochainement obligatoires, comme l'est l'exercice incendie. Nous lancerons au cours du 1er trimestre un nouvel appel d'offre pour pouvoir organiser d'autres exercices, avec la possibilité d'être accompagné en cas de crise réelle. Ce marché sera cohérent avec les actions portées par l'ANS dans le cadre du Groupe de Travail Territorial Cybersécurité dont SESAN est sponsor(**). Un nouveau marché de tests d'intrusion est en préparation, afin de tester la résistance de vos SI. D'autres actions sont en cours, nous vous les présenterons dans les prochains mois.

Notre réseau d'échange et de partage (<https://sesan.jamespot.pro>) vous permet de solliciter vos homologues en Ile-de-France et de nous remonter vos besoins et vos questions. N'hésitez pas à en (ab)user !

Notre force est dans la mutualisation et la coopération : plus nous sommes nombreux, plus nous serons efficaces. Rejoignez-nous sur tous ces projets, et invitez vos homologues pas encore adhérents à nous contacter : une seule adresse ssi@sesan.fr !

(*) 7 exercices réalisés - Un retour d'expérience sera présenté au congrès de l'APSSIS du 5 au 7 avril ; (**) avec le GRADeS Pays-de-Loire, la région Bourgogne Franche-Comté et la Réunion

INFORMATION



ESMS numérique: Projets de déploiement du dossier usager informatisé financés à hauteur de 12,2 millions d'euros [>>Lire l'article](#)

La Caisse nationale de solidarité pour l'autonomie (CNSA), dans une décision publiée le 31 décembre, détaille la répartition aux agences régionales de santé (ARS) des 12,2 millions d'euros de crédits 2021 du Ségur du numérique en santé alloués au financement des 10 projets lauréats de l'appel national visant à encourager les établissements sociaux et médico-sociaux (ESMS) à déployer une solution de dossier usager informatisé.

TIC SANTE, 03/01/2022

Nouvelle fuite de données santé de français, cette fois le pirate rajoute des données bancaires. [>>Lire l'article](#)

ZATAZ découvre une nouvelle fuite de données santé touchant des milliers de français, utilisateurs d'un service de téléassistance. En plus des feuilles de soin, le pirate rajoute la copie des pièces d'identité et les données bancaires d'abonnés.

ZATAZ, 05/01/2022

Le Gouvernement met le Health Data Hub en pause [>>Lire l'article](#)

Le gouvernement français a retiré une demande d'autorisation auprès de la Cnil pour le Health Data Hub afin d'héberger la base principale du système national des données de santé. L'hébergement de ce projet sur Azure de Microsoft est critiqué par des associations et des parlementaires

LE MONDE INFORMATIQUE, 07/01/2022

La cyber sécurité, un enjeu majeur de la présidence française de l'Union européenne [>>Lire l'article](#)

Pour sa présidence du Conseil de l'Union européenne, lors du premier semestre 2022, la France fait la cybersécurité l'un de ses axes de travail prioritaires. Les chantiers sont nombreux : réviser la directive NIS sur les opérateurs de services essentiels, éprouver la coopération entre les Etats membres en cas d'incidents cyber,...

USINE DIGITALE, 12/01/2022

BONNES PRATIQUES



OSE, SIE et analyse des risques EBIOS RM

[>>Lire l'article](#)

Les 135 Hôpitaux désignés Opérateurs de Services Essentiels (OSE) en 2021 ont défini et déclaré leurs Systèmes d'Informations Essentiels (SIE). La mise en œuvre opérationnelle des 23 règles de la Directive NIS I devient alors un chantier prioritaire, à mener selon un calendrier établi avec l'ANSSI.

DSIH, 10/01/2022

Test des procédures dégradées : que tester et jusqu'où ?

[>>Lire l'article](#)

Faut-il des procédures dégradées relatives au SI ? En termes techniques, c'est ce qu'on appelle un PCA-PRA : plan de continuité d'activité et plan de reprise d'activité.

DSIH, 18/01/2022

Pourquoi a-t-on intérêt à porter plainte en cas de cyberattaque ?

[>>Lire l'article](#)

La cybercriminalité fait chaque semaine la une de l'actualité, avec des agresseurs qui semblent furtifs et intouchables. Pourtant, le dépôt de plainte de la part des entités victimes peut faire partie de la stratégie de résilience des organisations.

USINE DIGITALE 20/01/2022

MENACES



Une rançon demandée après la cyberattaque du Pôle Santé Vinci à Chambray-lès-Tours [>>Lire l'article](#)

Victime d'un piratage informatique depuis vendredi dernier, le Pôle Santé Léonard de Vinci à Chambray-lès-Tours fait face en réalité à une attaque par ransomware. Les pirates demandent une rançon pour rétablir les données de l'établissement, selon nos informations.

FRANCE BLEU, 10/01/2022

Vigilance face aux activités du groupe Mespinoza [>>Lire l'article](#)

Le 6 janvier 2022, le département de la Santé et des Services sociaux des États-Unis (HHS) a publié une alerte concernant un groupe cybercriminel connu en tant que Mespinoza. Actif depuis l'année 2018, ce groupe s'attaque au secteur gouvernemental, l'industrie, le domaine de l'éducation ainsi que le domaine de la santé

CYBERVEILLE SANTE, 20/01/2022

Retour de 500 000 données de santé piratés, + 100 000 autres. [>>Lire l'article](#)

500 000 données de santé piratées découvertes par ZATAZ en 2021 refont surface dans une boutique pirate. Un échantillon gratuit pour vendre d'autres données exfiltrées.

ZATAZ, 25/01/2022

Le ministère de la Justice victime d'un ransomware ? [>>Lire l'article](#)

Le ministère de la Justice aurait été victime d'une cyberattaque. Elle est revendiquée par le groupe criminel LockBit 2.0. Il dit détenir près de 8000 fichiers qu'il menace de publier le 10 février prochain si la rançon n'est pas versée.

USINE DIGITALE, 28/01/2022

VULNÉRABILITÉ



Vulnérabilité dans l'agent Cortex XDR de Palo Alto

[>>Lire l'article](#)

L'exploitation de cette vulnérabilité par un attaquant authentifié permet l'exécution de programmes malveillants avec des droits supérieurs.

CYBERVEILLE SANTE, 12/01/2022

75 % des prestataires de santé utilisent des équipements au système d'exploitation obsolète

[>>Lire l'article](#)

Selon le dernier rapport de Kaspersky sur le secteur de la santé, seulement 20 % des prestataires de santé européens - et 10 % des Français - assurent que leurs équipements utilisent les dernières versions logicielles.

GLOBAL SECURITY MAG, 25/01/2022

RGPD/ JURIDIQUE



Accès aux données médicales : quand la Cour de Cassation rappelle qu'il n'y a pas que le RGPD dans la vie

[>>Lire l'article](#)

Difficile aujourd'hui de ne pas évoquer le « RGPD » quand il est question de données à caractère personnel, et de données de santé. Pourtant, l'encadrement et la protection des données de santé ne s'arrête pas qu'à ce règlement européen.

VILLAGE JUSTICE, 04/01/2022

La CNIL organise une consultation publique sur la modification des méthodologies de référence pour la recherche en santé

[>>Lire l'article](#)

La CNIL fait évoluer les méthodologies de référence (MR) 005 et 006 relatives aux traitements de données du Système national de données de santé (SNDS) à des fins de recherches, d'études ou d'évaluation dans le domaine de la santé. Elle organise une concertation avec les acteurs concernés par ces évolutions jusqu'au 18 février 2022.

CNIL 10/01/2022

Vidéosurveillance : la difficile conciliation de la protection des données et du droit à la preuve de l'employeur

[>>Lire l'article](#)

Dans un arrêt en date du 10 novembre 2021 (publié au bulletin), la Chambre sociale de la Cour de cassation procède à un rappel utile des règles applicables en matière d'utilisation d'éléments de preuve obtenus au moyen d'un dispositif de vidéosurveillance sur le lieu de travail. En l'espèce, un système de vidéosurveillance avait été mis en place au sein d'une pharmacie située à Mayotte. Constatant, grâce aux enregistrements de la vidéosurveillance, qu'une salariée avait commis une faute.

LEXPLICITE, 21/01/2022

Publication de l'Index AFCDP 2022 du Droit d'accès

[>>Lire l'article](#)

Comme chaque année et quelques jours avant la journée européenne de la protection des données, l'AFCDP, l'association des Délégués à la protection des données (DPD/DPO) et autres professionnels de la protection des données, publie son « Index annuel du Droit d'accès ».

GLOBAL SECURITY MAG, 25/01/2022