NEWSLETTER SSI SESAN

Bonjour à toutes et à tous,

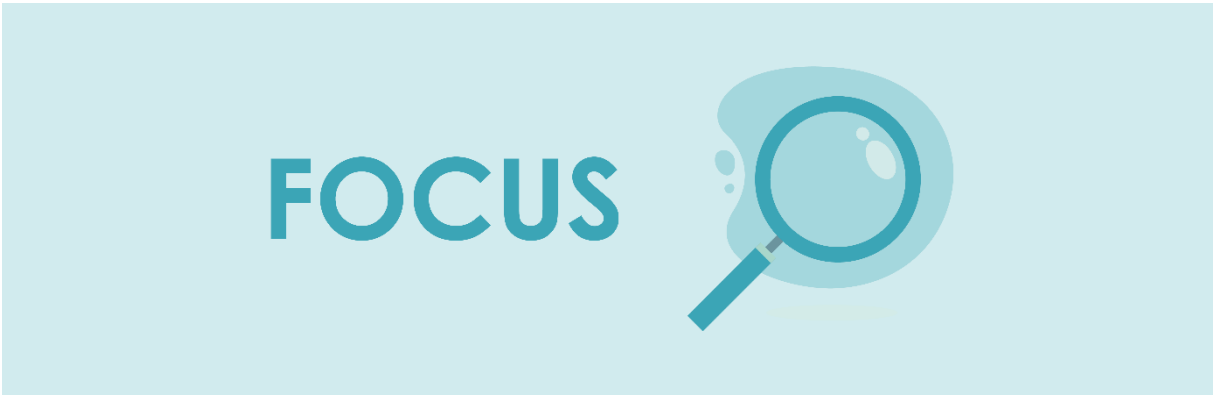
Le cybermois 2022 s'est achevé sur la publication de ***l'arrêté du 26/10/2022*** *relatif à l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics(1). En plus du rappel de la déclaration obligatoire des incidents de sécurité, le point 5.2 rappelle que « le dirigeant exécutif de l'établissement s'assure de la définition et de la mise en œuvre d'une organisation adaptée pour assurer la sécurité numérique des systèmes d'information et de communication ». Le message est clair,* ***la sécurité n'est pas qu'une affaire de DSI !***

Nous vous donnons rendez-vous le 8 novembre pour ***la journée régionale dédiée à la e-Santé****(2), avec une table ronde dédiée à la sécurité du système d'information et un stand spécifique où nous répondrons directement à vos questions.*

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

(1) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046503128

(2) https://www.sesan.fr/nos-actualites/sesan-organise-la-journee-de-la-esante-en-ile-de-france-le-8-novembre



Cyber-assurance : entre mobilisation et critique *>>Lire l'article*

Plusieurs grandes entreprises ont décidé de créer leur propre assurance pour couvrir les cyber-risques. Dans le même temps, les membres du Cesin ont manifesté leur opposition au projet gouvernemental d'indemniser les victimes de rançons par les assureurs à condition de déposer plainte.

LMI, 04/10/2022

Le paiement des rançons 2.0 *>>Lire l'article*

Les menaces et les attaques sont en effet de plus en plus nombreuses mais, surtout, de plus en plus violentes. Les organisations sont aujourd'hui confrontées au phénomène de ransomware, un logiciel informatique malveillant qui prend en otage les données et réclame le paiement d'une rançon. Faut-il ou non céder et payer la somme demandée ? Eléments de réponse.

CYBERSECURITY GUIDE, 17/10/2022

Chaos dans six hôpitaux de Barcelone suite à une attaque informatique >>Lire l'article

Six centres de soins de la capitale catalane et de la région métropolitaine de Barcelone en prise avec des cyber attaques. Ils ne peuvent plus prendre de rendez-vous, passer des tests médicaux ou s'occuper de patients.

ZATAZ, 07/10/2022

Santé : une majorité d'organisations du secteur a déjà été victime d'un rançongiciel au cours des trois dernières années >>Lire l'article

Le constat est unanime : les attaquants cherchent à affaiblir les organisations de santé et utilisent massivement les attaques par rançongiciels : 86 % d'entre elles ont déjà été compromises par ce type d'attaque et ont subi de réels dysfonctionnements dans leur fonctionnement opérationnel.

ITCHANNEL, 13/10/2022

CERT Santé – Mise en place d'une permanence de son service de réponse à incident 24h/24 >>Lire l'article

A partir du 17 octobre 2022, le CERT Santé étend son service de réponse à incident aux heures non ouvrées. Une astreinte est mise en place pour accompagner les bénéficiaires du CERT Santé confronté à un incident majeur ayant déjà affecté un ou plusieurs services numériques et contraignant l'établissement à mettre en place un mode dégradé de fonctionnement.

CYBERVEILLE SANTE, 14/10/2022

La météo n'est pas très bonne : alerte le directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information *>>Lire l'article*

Les cyberattaques de réseaux informatiques, d'entreprises ou encore d'hôpitaux contre rançon se multiplient et l'espionnage se développe, ont constaté les Assises de la cybersécurité, qui se sont déroulées jusqu'à vendredi à Monaco.

FRANCE INFO, 15/10/2022

Compte rendu des 2èmes Rencontres SSI Santé *>>Lire l'article*

Ces rencontres ont réuni une centaine de participants impliqués dans le domaine de la sécurité des données de santé. Des directeurs de la sécurité des données numériques, des experts cybersécurité, des juristes, et d'autres spécialistes.

APSSIS, 24/10/2022

BONNES PRATIQUES

Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité

>>Lire l'article

Dans un contexte de multiplication des compromissions de bases de mots de passe, la CNIL met à jour sa recommandation de 2017 pour tenir compte de l'évolution des connaissances et permettre aux organismes de garantir un niveau de sécurité minimal pour cette méthode d'authentification.

CNIL, 17/10/2022

MENACES

Que signifie « supply chain attack » ? Un cyber-agression redoutable *>>Lire l'article*

En français, on parle d'« attaques par la chaîne d'approvisionnement » ou par la chaîne logistique. Les supply chain-attacks passent par les systèmes informatiques des prestataires de l'entreprise visée, ce qui les rend ardues à repérer.

NUMERAMA, 23/10/2022

Etablissements de santé : la CISA émet une alerte au sujet du gang de ransomware Daixin Team *>>Lire l'article*

Plusieurs agences américaines, dont la CISA, ont publié une alerte de sécurité au sujet d'un groupe de cybercriminels nommés Daixin Team qui est à l'origine de nombreuses attaques informatiques ! Ce gang privilégie les attaques contre les établissements de santé et il a déjà fait plusieurs victimes aux États-Unis.

IT-CONNECT, 25/10/2022

Vulnérabilité dans Microsoft Edge [>>Lire l'article]

Une vulnérabilité dans le navigateur Microsoft Edge permet à un attaquant, en persuadant sa victime à visiter un site contenant des données spécifiquement forgées, de mener une attaque du type spoofing.

CYBERVEILLE SANTE, 06/10/2022

Fuite de données chez Microsoft [>>Lire l'article]

À cause de la mauvaise configuration d'un serveur, des informations sensibles de clients Microsoft ont été exposées sur Internet. Au total, 65 000 entreprises sont concernées.

IT-CONNECT, 20/10/2022

"Admin", "123456": ces mots de passe protégeant vos accès à distance bien trop vulnérables [>>Lire l'article]

Les attaquants ciblent d'abord des mots de faibles quand ils tentent de forcer les accès à distance RDP et SSH. Une tactique qui doit être prise en compte par les responsables sécurité.

ZDNET, 21/10/2022

Vulnérabilités critiques du 17/10/22 au 21/10/22 [>>Lire l'article]

Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine passée 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, 24/10/2022

RGPD/ JURIDIQUE

Cyber Resilience Act (CRA) : définition, obligations et sanctions >>Lire l'article

En parallèle de la refonte de la directive « Network and Information Security » (NIS), la présidente de la commission européenne avait annoncé en septembre 2021 la préparation d'un nouvel acte législatif sur la cyber-résilience, le « Cyber Resilience Act » (CRA)..

HAAS AVOCATS, 03/10/2022

Prudence sur Internet avec la CNIL >>Lire l'article

Une vidéo pour comprendre ce qu'est une donnée personnelle et le rôle de la CNIL.

CNIL, 14/10/2022

Usurpation d'identité : quelles solutions juridiques après en avoir subi une ? >>Lire l'article

Dans ce contexte où chacun peut être victime de piratage, il est important de connaitre les contours de l'usurpation d'identité, à savoir, sa définition, son champ d'application et les sanctions y attachées, pour ainsi pouvoir l'identifier et agir, d'une part, en amont avec l'emploi de moyens préventifs permettant d'éviter la commission de l'infraction, et d'autre part, en aval avec les solutions offertes aux victimes.

VILLAGE JUSTICE, 25/10/2022