n°37
Avril 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

JOURNÉE DE LA CYBERSÉCURITÉ

18 Avril 2023

De 9h à 17h30
Au Beffroi, 2 place Emile Cresp
92120 Montrouge

Nous vous donnons rendez-vous le **18 avril 2023** au Beffroi de Montrouge pour notre première journée de la cybersécurité en santé en Île-de-France.

Au programme :

Matin	• Cybersécurité, les enjeux en Île-de-France - ARS Île-de-France et SESAN • Conférence du CERT-Santé • Conférence de la Task Force Cyber : organisation, projets, orientation 2023 – 2027, … - Membres de la Task Force
Après-midi, 3 ateliers participatifs (inscription sur place)	• Cyberattaque, prendrez-vous les bonnes décisions ? • RSSI, DSI et Biomédical : une exigence d'entente ! • Cybersécurité: un sujet de direction générale

Conclusion par l'ANSSI

Pour vous inscrire (il reste quelques places) :
https://www.eventbrite.fr/e/billets-journee-de-la-cybersecurite-en-ile-de-france-542993045817

Un doute ?

Une question ?

Contactez-nous sur
ssi@sesan.fr

Actus à la une

UNE AUTRE MÉTHODE D'ÉVALUATION DE LA VRAISEMBLANCE

Ce document présente une méthode d'évaluation de la vraisemblance des scénarios opérationnels différente de celle proposée dans les fiches méthodes publiées par l'ANSSI.

CLUB EBIOS, 08/03/2023

Lire l'article

HOP'EN, SUN-ES et SONS : la DGOS a présenté son point d'étape

L'agence du numérique en santé (ANS) a organisé les 14 et 15 mars à Paris ses troisièmes Journées nationales du numérique à l'hôpital. Elles ont été l'occasion de présenter le chemin parcouru par les programmes HOP'EN et SUN-ES dédiés à la transformation numérique et la modernisation des établissements de santé.

DSIH, 15/03/2023

Lire l'article

Femmes, Numérique et Cyber [ETUDE]

L'enquête d'Anna Pujol-Mazzini pour l'APSSIS dresse un état des lieux sans concession sur la place des femmes dans l'écosystème du numérique. En fin de dossier, et comme une synthèse de bonnes pratiques, vous trouverez la "checklist pour recruter plus de femmes dans le numérique".

APSSIS, 27/03/2023

Lire l'article

Bonnes pratiques

Cellule de crise SSI : qui mobiliser ?

Le nombre de cyber-attaques touchant les établissements de santé reste au plus haut niveau. Alors que faire face à cette situation ? La réponse : se préparer aux intempéries à venir !

DSIH, 20/03/2023

Lire l'article

Kaspersky met à disposition l'outil de déchiffrement d'un variant de Conti

Le 16 mars 2023, Kaspersky a publié un outil de déchiffrement ciblant un variant du rançongiciel Conti. Ce logiciel permet aux entreprises ayant subi une attaque par ce groupe de récupérer leurs données.

CYBERVEILLE, 24/03/2023

Lire l'article

Faire évoluer la cybersécurité vers un état d'esprit axé sur la prévention*

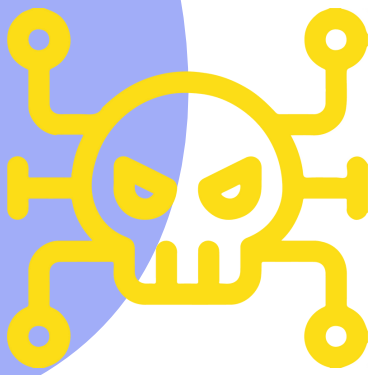
Le coût d'une violation de données peut être bien plus important que l'investissement dans la prévention. Selon une étude d'IBM, le coût moyen d'une violation de données en 2022 était de 4,35 millions de dollars .

FORBES, 26/03/2023

Lire l'article

**Article en anglais*

Menaces



Plusieurs hôpitaux européens victimes de cyberattaques

Des établissements hospitaliers à Brest, Bruxelles ou encore Barcelone ont été récemment touchés par une attaque informatique.

Lire l'article

ORANGE, 12/03/2023

Arnaque au président : récit d'une attaque menée en moins de 3 h

Lire l'article

Les équipes de Microsoft viennent de détailler la chronologie d'une cyberattaque en compromission d'e-mail professionnel menée en l'espace de quelques heures seulement.

LEMAGIT, 13/03/2023

Les Anonymous Soudanais s'attaquent à la France !

Après avoir visé les aéroports, des hackers ont attaqué une trentaine d'hôpitaux et d'universités françaises, ainsi que l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Lire l'article

ZATAZ, 17/03/2023

Menaces

Bloquer les scanners à la découverte de votre exposition sur Internet : bonne ou mauvaise idée ?

Lire l'article

L'auteur présente les avantages et inconvénients du blocage des scanners, et suggère plutôt de minimiser l'exposition des données et d'adopter des pratiques de sécurité solides. Enfin, il souligne l'importance de la collaboration entre chercheurs et organisations pour renforcer la sécurité en ligne.

DSIH, 21/03/2023

ChatGPT : attention, n'importe qui peut voir vos conversations, OpenAI coupe l'accès au service en urgence

Lire l'article

ChatGPT est victime d'un bug épineux en ce début de semaine. Celui-ci dévoilait les descriptions de vos conversations avec l'IA aux autres utilisateurs. En attendant de résoudre le problème, OpenAI a tout bonnement désactivé l'historique des chats.

TOM'S GUIDE, 23/03/2023

Juridique

Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne

Lire l'article

Le 28 février, le Comité européen à la protection des données (CEPD) a rendu son avis sur le projet de décision d'adéquation de la Commission européenne. Il relève les améliorations apportées par le nouveau cadre juridique américain, mais indique que des préoccupations subsistent.

CNIL, 01/03/2023

Données de santé : la CNIL rappelle à deux organismes de recherche médicale leurs obligations légales

Lire l'article

La présidente de la CNIL a rappelé à deux organismes procédant à des recherches médicales leurs obligations de réaliser une analyse d'impact sur la protection des données et d'informer correctement les personnes.

CNIL, 13/03/2023

Communauté

Question du mois :

"Comment sécuriser l'accès à distance de ses prestataires ?"

La sécurisation de l'accès à distance pour les fournisseurs de services est une préoccupation majeure pour de nombreuses organisations qui externalisent les services informatiques. Vous pouvez prendre plusieurs mesures pour protéger cet accès.

Voici quelques étapes à suivre :

1 **Établir une politique d'accès à distance :**
Une politique d'accès à distance définit des directives pour un accès à distance sécurisé à un système. Assurez-vous que tous les fournisseurs de services connaissent et respectent cette politique. (Par exemple : activer le compte sur demande, utiliser une adresse IP publique, terminer l'installation de l'application sur demande, utiliser le compte administrateur local de la machine cible, etc.)

2 **Utiliser l'authentification à deux facteurs (2FA) :**
Obligez les fournisseurs de services à utiliser l'authentification à deux facteurs pour l'accès à distance. Cela ajoute une couche de sécurité supplémentaire au processus d'authentification et réduit le risque d'accès non autorisé.

3 **Mettre en place un réseau privé virtuel (VPN) ou un bastion :**
Un VPN fournit une connexion sécurisée entre l'appareil du fournisseur de services et le réseau de votre organisation, ce qui rend plus difficile l'interception des données par les pirates.

Par contre, le VPN a ces limites.

- Si un attaquant accède aux identifiants VPN d'un employé distant, il pourra accéder à toutes les applications et données du réseau correspondant.
- Ils peuvent parfois ralentir la connexion internet et la rendre instable.
- L'installation d'un agent est obligatoire,
- Vos journaux de connexion et registres d'activités (logs) ne sont plus détenus par votre fournisseur d'accès à Internet mais par le prestataire VPN.

Le bastion d'administration cloisonne les accès entre les différentes ressources disponibles sur le réseau, suit toutes les actions des comptes supervisés, voire pour certaines, enregistre l'écran et la session. Il fournit la traçabilité des accès.

4 **Limitez l'accès à des ressources spécifiques :**
Les prestataires de services ne devraient avoir accès qu'aux ressources spécifiques dont ils ont besoin pour accomplir leurs tâches. Cela permet de réduire le risque de violation de données causée par des informations d'identification compromises.

Communauté

5 **Contrôlez les flux :**
Pour les flux spécifiques (laboratoire, remontée d'information,...), créez une liste blanche s'il y a une nécessité.

6 **Contrôler et enregistrer tous les accès à distance (LOGS) :**
Surveiller et enregistrer toutes les activités d'accès à distance des prestataires de services. Cela permet de détecter les tentatives d'accès non autorisé et d'y répondre rapidement. Il est nécessaire d'avoir une attention particulière sur les points suivants :

- Les tentatives d'accès échouées,
- Les accès en HNO (Heures Non Ouvrables),
- Le changement de mot de passe des comptes à privilèges en HNO.

7 **Réviser et mettre à jour régulièrement les protocoles de sécurité et les comptes d'accès :**
Réviser et mettre à jour régulièrement les protocoles de sécurité pour s'assurer qu'ils restent efficaces face aux nouvelles menaces. En parallèle, faite une révision régulière des comptes d'accès et d'habilitations en fonction de la criticité du SI, de manière mensuelle à semestrielle.

En utilisant ces mesures, vous pouvez sécuriser l'accès à distance de vos prestataires et protéger vos données sensibles.

Nous vous invitons à consulter le guide réalisé par Agence du Numérique en Santé :
https://www.cyberveille-sante.gouv.fr/

Une question?

ILE-DE-FRANCE
sesan
Groupement d'Intérêt Public **eSanté**