n°36
Mars 2023

esesan
Groupement d'Intérêt Public eSanté

Newsletter Cybersanté

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

TOUS CYBER VIGILANTS

Edito

Le 16 février, le HC3 a publié un bulletin sur la menace de 2022 et les attentes pour l'année à venir (1).
Le rapport (2) indique que les attaques par rançongiciel vont se poursuivre et préconise des actions de prévention qui rejoignent celles présentées dans la précédente Newsletter.

Les services SESAN de cybersécurité sont bien une partie de la réponse. Nous allons continuer à faire évoluer notre offre dans les prochains mois afin de mieux préparer et protéger tous les établissements franciliens.

Un exercice de cybercrise est une bonne approche pour évaluer votre capacité de réaction. L'Appel à projet de l'ARS IDF (3) et le marché SESAN vous permettent de faire un exercice basé sur les kits ANS (4).

Sources :

1. *https://www.cyberveille-sante.gouv.fr/actualites/etats-unis-le-hc3-publie-un-bulletin-sur-la-menace-de-2022-et-les-attentes-pour-lannee*
2. *https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf*
3. *https://www.iledefrance.ars.sante.fr/lancement-dun-appel-projet-visant-le-financement-dun-exercice-de-continuite-dactivite-au-profit-des*
4. *https://www.cyberveille-sante.gouv.fr/dossier-thematique/exercice-de-crise-cyber*

Un doute ?

Une question ?

Contactez-nous sur
ssi@sesan.fr

Actus à la une

ENISA dévoile son nouvel outil de sensibilisation AR-in-a-Box*

AR-in-a-Box est une solution complète pour les activités de sensibilisation à la cybersécurité conçue pour répondre aux besoins des organismes publics, des opérateurs de services essentiels et des grandes et petites entreprises privées. Il fournit des connaissances théoriques et pratiques sur la façon de concevoir et de mettre en œuvre des programmes efficaces de sensibilisation à la cybersécurité.

Lire l'article

ENISA, 06/02/2023

**Supports disponibles en anglais*

Replays de 3 conférences du CLUSIF

"23e Panocrim" : bilan annuel en matière de cybercriminalité

"De la crise cyber à la crise systémique"

"OT : menaces cyber et réponses"

Lire l'article

CLUSIF, 10/02/2023

Agir au cœur des territoires pour la sécurité numérique

En synergie avec les structures et les autorités régionales existantes, l'ANSSI développe depuis plusieurs années des dispositifs visant à soutenir le tissu économique et les institutions à l'échelle régionale face à la menace cyber.

Lire l'article

ANSSI, 22/02/2023

Bonnes pratiques

Conférence de clôture de l’exercice REMPAR22

L’ANSSI met à disposition des organisations une collection de guides « Gestion de Crise Cyber » afin de leur permettre de progresser dans la gestion des crises d’origine cyber

ANSSI, 14/02/2023

Lire l'article

Le rôle des RSSI dans la gestion de communication post-cyberattaque

Lire l'article

Les RSSI doivent prendre l'initiative d'élaborer un plan de communication post-cyberattaque qui informe précisément les parties prenantes et suscite la confiance au sein de l'entreprise.

LMI, 16/02/2023

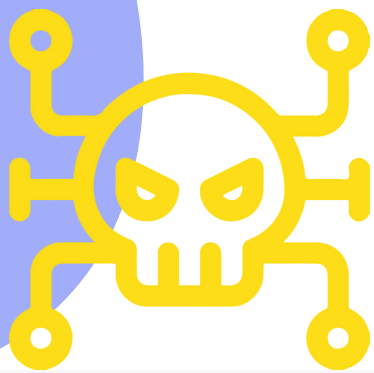
Protéger les hôpitaux grâce aux technologies réseaux (NDR)

Aider les établissements de santé à maitriser le risque cyber nécessite d’adopter une approche résolument proactive en prenant en compte les contraintes propres au secteur. La protection du réseau – et les technologies adaptées – sont indispensables pour prémunir les structures concernées.

DSIH, 24/02/2023

Lire l'article

Menaces



Le Groupe KillNet vise le secteur de la santé

Le 30 janvier 2023, le HC3 a publié une alerte concernant une campagne d'attaques menée contre le secteur de la santé par le groupe hacktivisite russophone KillNet, connu pour ses attaques de type DDOS (déni de service distribué). Actif depuis 2012, leurs activités se sont intensifiées depuis le début du conflit ukrainien.

Lire l'article

Cyberveille-santé, 03/02/2023

Une vague d'attaques par ransomware cible les failles du logiciel VMware ESXi

Lire l'article

Des milliers des machines ont été touchées par un ransomware s'en prenant au logiciel VMware ESXi, aussi bien en France qu'outre-Atlantique. La faille était pourtant connue depuis deux ans, mais toutes les mises à jour n'avaient pas été faites.

USINE DIGITALE, 07/02/2023

ZATAZ » LockBit 3.1 : déjà plus de 200 victimes en 2023

Malgré l'arrestation de l'un de ses membres, le 26 octobre 2022 au Canada, le groupe de hackers malveillants, LockBit, n'a jamais été aussi présent dans les machines des entreprises.

Lire l'article

ZATAZ, 13/02/2023

Juridique

Demandes d’autorisation en santé : la CNIL publie les critères à respecter

La CNIL publie deux fiches guidant les responsables de traitement dans le dépôt de leurs demandes d’autorisation de traitements dans le domaine de la santé (pour la recherche et hors recherche). Ces fiches déroulent les questions à se poser ainsi que les pièces à joindre au dossier de demande.

Lire l'article

CNIL, 06/02/2023

Incendie OVH : une première décision de condamnation

Lire l'article

Le tribunal juge qu’en stockant les 3 réplications de sauvegarde au même endroit que le serveur principal, OVH engage sa responsabilité contractuelle au titre du contrat de sauvegarde.

ULYS, 07/02/2023

Les DPO plus que jamais embarqués dans la cybersécurité

Lire l'article

L'Association Française des Correspondants en Données Personnelles (AFCDP) a tenu à la Maison de la Chimie (Paris) la 7e édition de son Université. La cybersécurité reste bel et bien au cœur du métier des DPO.

LMI, 09/02/2023

Communauté

Question du mois

"Quelles sont les meilleures pratiques de sécurité à mettre en place lors de l'externalisation des systèmes de santé numérique (application métier, mails, etc.) ?"

L'externalisation des systèmes de santé numériques est de plus en plus courante dans l'industrie médicale, et cette externalisation est appelée infogérance. Cependant, cela peut entraîner des risques de sécurité importants en termes d'intégrité, de disponibilité, de confidentialité et de traçabilité. Voici quelques bonnes pratiques de sécurité à mettre en œuvre lors de l'externalisation des systèmes de santé numériques :

1 Effectuer une évaluation complète des risques :

Avant d'externaliser, effectuez une évaluation complète des risques associés à l'externalisation de votre système de santé numérique, notamment les risques liés à la sécurité, à la confidentialité, à la conformité et identifier les vulnérabilités potentielles qui pourraient être exploitées. Cela vous aidera à déterminer les solutions de prestataires qui répondent le mieux à vos besoins et quelles mesures de sécurité sont nécessaires pour protéger votre système de santé numérique. Mettez en place un Plan d'Assurance Sécurité (PAS) entre vous et le prestataire.

2 Avoir un fournisseur certifié/recommandé par l'ANSSI :

Assurez-vous que ce fournisseur (cloud, EDR/XDR, SOC, sécurité des emails...) est certifié ou recommandé par l'ANSSI. Vérifiez si celui-ci a les certifications : HDS1, ISO 270012, ISO 277013, les audits et politiques de sécurité appliquées (chiffrement des données, mécanismes d'authentification multi-facteurs, contrôles d'accès basés sur les rôles, etc.).

Définissez le niveau de service attendu et les garanties associées avec les garanties suivantes :

- SLA : Définit les attentes du client et les engagements du prestataire à y répondre.
- PSG : Définit le cadre temporel de disponibilité de service et donc de prise en charge des garanties.
- GTI : Définit le délai d'intervention du prestataire suite à un incident.
- GTR : Définit le temps maximum dont dispose le prestataire pour rétablir le service informatique après un incident technique.
- PAS : A pour but de préciser comment les prestataires se conforment aux exigences de cybersécurité.
- PAQ : Définit les objectifs du projet, la façon dont on va procéder : étapes, conditions... et le processus mis en œuvre.

Ces garanties définissent et stipule les exigences de sécurité, la responsabilité du fournisseur et les mesures de sécurité à mettre en place. Vous pouvez également évaluer l'historique de sécurité en recherchant des informations sur des compromissions passées.

Communauté

- EDR/XDR/SOC : https://experiences.microsoft.fr/articles/cybersecurite/edr-et-xdr/
- SLA/PSG/GTI/GTR : https://www.wifirst.com/
- PAS : https://www.makeitsafe.fr/comment-elaborer-un-plan-dassurance-securite-pas-pour-lexternalisation/
- PAQ : https://www.bluesoft-group.com/qu-est-ce-qu-un-paq/

3 Mettre en place un plan de continuité ou de reprise d'activité :

Il est important de s'assurer qu'un plan de continuité ou de reprise après sinistre est en place en cas de violation de données ou de défaillance du système. Testez et mettez à jour ce plan régulièrement pour assurer une exécution sans heurts en cas d'urgence.

4 Sensibiliser les employés aux bonnes pratiques de sécurité :

Enfin, assurez-vous que les employés qui ont accès à des données sensibles connaissent les bonnes pratiques de sécurité et reçoivent régulièrement une formation en matière de sécurité. Cela empêchera les failles de sécurité accidentelles dues à une erreur humaine.

Ces pratiques de sécurité vont contribuer à protéger votre système de santé numérique contre les menaces de sécurité et à contribuer à assurer la confidentialité, la disponibilité et la sécurité des données lors de l'externalisation de votre système de santé numérique.

Nous vous invitons à consulter le guide réalisé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf

Une question?

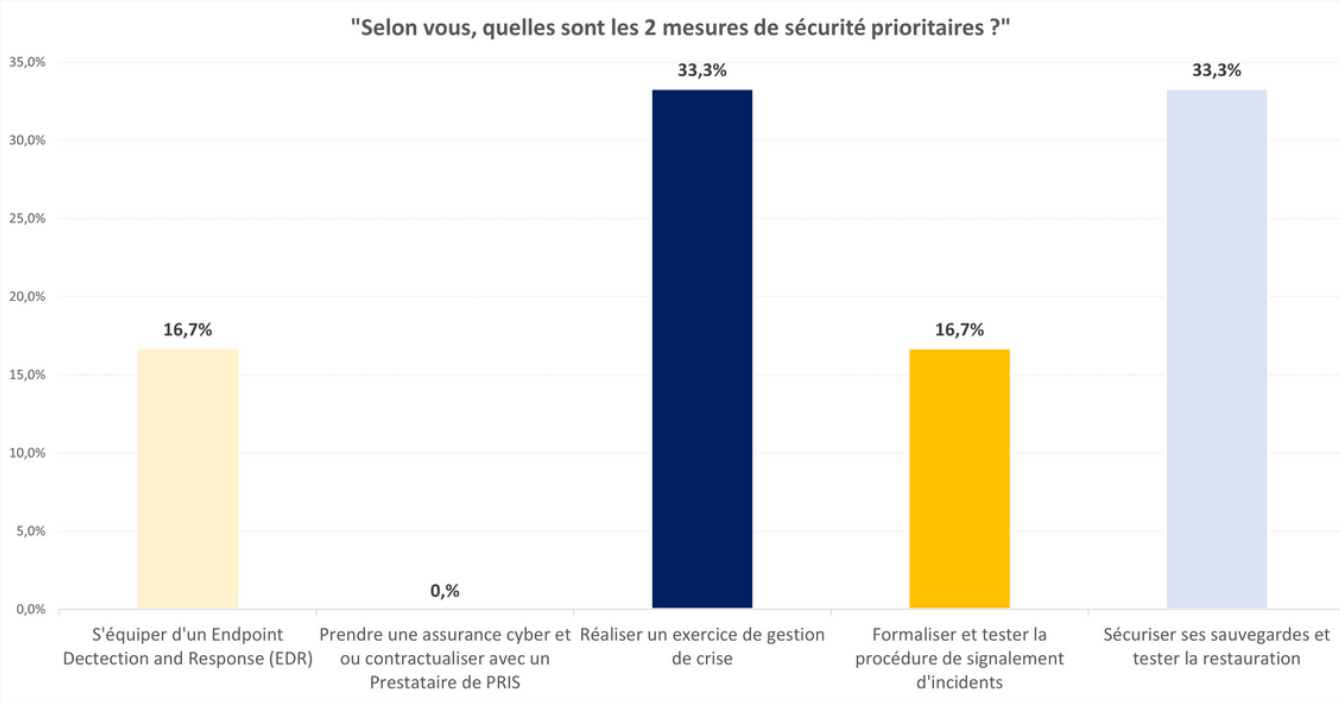
Sondage du mois

Répondre

Pensez-vous faire un exercice de cybercrise en 2023 ?

Communauté

Résultats du sondage du mois dernier




sesan
Groupement d'Intérêt Public eSanté