NEWSLETTER SSI SESAN

Bonjour à toutes et tous,

Des menaces, encore des menaces, toujours des menaces : les mois se suivent et se ressemblent. Encore de nouvelles fuites de données et de « nouvelles » attaques en ce mois de mars. Cette fois, des personnes non autorisées ont utilisé des ***comptes Amelipro compromis pour exfiltrer les données de 510 000 assurés*** *(1). L'Assurance Maladie a heureusement rapidement détecté ce piratage et informé chaque personne concernée.* ***Outre atlantique, ce sont des onduleurs qui se retrouvent mis en lumière*** *: afin de faciliter la maintenance, certains constructeurs ont intégré des capteurs permettant la remontée d'information. Problème : cet accès peut aussi servir à se connecter à la ressource avec une interface classique login/mot de passe laissés parfois aux valeurs par défaut (2). Pensez à changer les mots de passe par défaut sur vos équipements connectés !*

Dans le cadre du SEGUR, l'ARS IDF a confié à SESAN la déclinaison opérationnelle de la cybersécurité *sur la région Ile-de-France. Des informations (dont cette Newsletter) seront régulièrement publiées sur https://segurnumerique.sante-idf.fr/animation-regionale/cybersecurite/.*

Le 31 mars, c'est ***la journée mondiale de la sauvegarde des données informatiques*** *(3). L'occasion de rappeler à tous l'importance de faire des sauvegarde ET de les tester : si vous ne disposez pas d'un environnement pour tout restaurer, assurez-vous que vous pouvez recharger un fichier « témoin ». Cela permet a minima de contrôler la réalité de la sauvegarde (taille > 0 octets) et de sa capacité à la relire.*

Un sujet vous intéresse, vous souhaitez découvrir tous nos services et solutions : contactez-nous sur ssi@sesan.fr !

(1) https://assurance-maladie.ameli.fr/presse/2022-03-17-infopresse-connexions-non-autorisees-comptes-amel

(2) https://www.cisa.gov/uscert/ncas/current-activity/2022/03/29/mitigating-attacks-against-uninterruptable-power-supply-devices

(3) https://www.cybermalveillance.gouv.fr/tous-nos-contenus/evenements/journee-mondiale-de-la-sauvegarde-des-donnees-informatiques

Rapport HelpNetSecurity : état des lieux de la cybersécurité dans le monde de la santé >>Lire l'article

Selon ce rapport, il y a eu en 2021 quelques 679 fuites de données de santé. De plus, ces attaques ont augmenté de 35% par rapport à l'année précédente. Les organismes de santé sont en effet des cibles privilégiées pour les attaquants du fait de la valeur de leurs données, mais également du manque de protection de leur réseau.

CYBERVEILLE SANTE, 07/03/2022

Panorama de la menace informatique 2021 >>Lire l'article

Dans ce panorama de la menace informatique, l'ANSSI revient sur les grandes tendances ayant marqué le paysage cyber sur l'année 2020-2021 et en propose des perspectives d'évolution à court terme. Ces tendances s'inscrivent dans une hausse continue du niveau de menace.

ANSSI, 09/03/2022

Doctolib va davantage mettre l'accent sur la cybersécurité >>Lire l'article

La plateforme de rendez-vous médicaux annonce une nouvelle levée de fonds de 500 millions. De quoi valoriser l'entreprise française à hauteur de 5,8 milliards d'euros. Doctolib souhaite recruter 3 500 personnes dans les cinq prochaines années, et renforcer sa sécurité.

ZDNET, 16/03/2022

TOP 10 des vulnérabilités 2021 *>>Lire l'article*

Analyse des vulnérabilités les plus critiques traitées par l'ANSSI au cours de l'année 2021. Cette démarche s'inscrit dans les missions de sécurité et de défense des systèmes d'information de l'agence, et en particulier la mission de veille et d'information sur les vulnérabilités.

ANSSI, 22/02/2022

SEGUR NUMERIQUE : Cyber sécurité en région *>>Lire l'article*

Les régions organisent leur action autour d'un Plan de renforcement de la cybersécurité.

SEGUR NUMERIQUE, 01/03/2022

MENACES

Connexion de personnes non autorisées à des comptes amelipro *>>Lire l'article*

l'Assurance Maladie a détecté que des personnes non autorisées ont réussi à se connecter à des comptes amelipro, réservés aux professionnels de santé. Il ressort des premières analyses que les attaquants ont pu se connecter à des comptes dont les adresses e-mail avaient été compromises : 19 comptes de professionnels de santé ont été identifiés.

ASSURANCE MALADIE, 17/03/2022

Le piratage d'Okta par Lapsus$ *>>Lire l'article*

Un chercheur en sécurité a mis la main sur un rapport forensique qui montre comment les pirates ont procédé.

01NET, 30/03/2022

L'hôpital de Castelluccio visé par une cyberattaque *>>Lire l'article*

L'hôpital de Castellucio fait face à une cyberattaque avec demande de rançon depuis lundi 28 mars. Les soins de radiothérapie et d'oncologie sont suspendus..

FRANCE3, 29/03/2022

Vulnérabilités critiques dans des produits Baxter [>>Lire l'article]

La société Palo Alto a publié le 2 mars 2022 une étude concernant les vulnérabilités de pompes à perfusion connectées. Une analyse des données provenant de plus de 200 000 pompes à perfusion connectées au réseau utilisées dans les établissements de santé a révélé que 75 % de ces dispositifs médicaux contiennent des failles de sécurité qui pourraient les exposer à un risque d'exploitation potentielle.

CYBERVEILLE SANTE, MAJ du 07/03/2022

Bulletin d'actualité du CERT-FR [>>Lire l'article]

Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine du 21 mars pour souligner leurs criticités.

CERT-FR, 28/03/2022

Vulnérabilité dans Chrome [>>Lire l'article]

Une vulnérabilité « confusion de type » dans le moteur V8 peut permettre une attaque par XSS. Un attaquant incitant un utilisateur à visiter un site web peut exécuter du code arbitraire sur son système.

CYBERVEILLE SANTE, 28/03/2022

RGPD/ JURIDIQUE

Data act : Bâtir l'avenir numérique de l'Europe [>>Lire l'article]

La proposition de règlement relatif à des règles harmonisées relatives à l'accès équitable aux données et à leur utilisation a été adoptée par la Commission le 23 février 2022. La loi sur les données est un pilier essentiel de la stratégie européenne en matière de données. Il apportera une contribution importante à l'objectif de transformation numérique de la décennie numérique.

COMISSION EUROPENNE, 04/03/2022

L'observabilité, indispensable à la sécurité des réseaux des organisations, contreviendrait-elle au RGPD ? [>>Lire l'article]

Appréhender et comprendre son réseau est devenu un impératif que les organisations ne peuvent plus ignorer. De ce fait, les outils d'observabilité des réseaux sont la clé pour anticiper les menaces et sécuriser la richesse informationnelle des entreprises ; notamment grâce au déchiffrement du trafic SSL/TLS, y compris les flux TLS 1.3. Dans un tel contexte, les organisations peuvent-elles vraiment respecter les réglementations relatives à la protection des données personnelles ?.

GLOBAL SECURITY MAG, 15/03/2022

Les arnaques RGPD [>>Lire l'article]

La CNIL a été informée d'une vague d'appels frauduleux ciblant particulièrement les pharmaciens. Des tentatives d'escroquerie sont régulièrement effectuées par des individus se faisant passer pour la CNIL. Que faire si vous êtes concerné ?

CNIL, MAJ du 29/03/2022

TRUCS ET ASTUCES

Je reçois des notifications indésirables sur ma e-CPS, que faire ? *>>Lire l'article*

Certains usurpateurs malveillants tentent d'abuser de la vigilance des professionnels de santé en déclenchant des notifications en espérant qu'ils les acceptent par réflexe ou pensant qu'il s'agit d'un collègue.

ANS, 01/03/2022

Et si la sensibilisation à la cybersécurité était aussi un jeu ? *>>Lire l'article*

la formation des collaborateurs aux enjeux, aux méthodes et aux principes de base de la cybersécurité gagne en importance et trouve un nouvel écho avec la gamification.

ZDNET, MAJ du 08/03/2022

Accompagnement Sécurité CERT Santé *>>Lire l'article*

De nombreux établissements ont été victimes de campagnes de rançongiciels depuis 2020. Les attaquants élèvent leurs privilèges et compromettent l'Active Directory et les sauvegardes et peuvent paralyser un établissement pendant plusieurs semaines. Afin d'accompagner les structures dans la mise en œuvre de mesures de protection face à cette menace, le CERT Santé a réalisé un support basé sur des recommandations issues des guides de l'ANSSI.

CERT SANTE, MAJ du 14/03/2022