

NEWSLETTER SSI SESAN



sesan

Bonjour à toutes et tous,

Après un début du mois de mai plutôt calme, nous nous attendions à le terminer sereinement. C'était sans compter sur les attaques durant le dernier long week-end avec des vagues de phishing, parfois ciblés. L'occasion de rappeler que **SESAN propose des tests de phishing pour sensibiliser les utilisateurs**. Ces tests répétés dans l'année permettent de réduire significativement le nombre de clics et de rappeler les bonnes pratiques.

A l'approche de l'été, le risque cyber augmente : moins de personnel dans les DSI et toujours autant de hackers. **Pour limiter les risques, nous proposons toujours un service de cybersurveillance 24x7**, pour détecter les fuites de données (**près de 500 comptes avec mot de passe retrouvés sur le Darknet en mai**) et les vulnérabilités de vos services exposés sur le net. **Pour sécuriser votre infrastructure interne, nous vous mettons à disposition un scanner de vulnérabilités** que vous pouvez opérer en toute autonomie.

Preuve que le sujet de la cyber est une priorité : **l'ENISA, l'agence européenne de sécurité des SI, organise en juin son exercice de cybercrise** qui a pour thème cette année la santé : plus d'informations sur <https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022>.

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

INFORMATION



Cybersécurité : quelles sont les 10 cybermalveillances les plus fréquentes ? [>>Lire l'article](#)

À ce jour, Cybermalveillance.gouv.fr référence 48 formes de cybermalveillances traitées par son outil d'assistance en ligne, qui permet aux victimes, en répondant à quelques questions, d'obtenir un diagnostic du problème rencontré et de disposer des conseils de cybersécurité permettant d'y faire face.

CYBERMALVEILLANCE, 12/04/2022

[Etats-Unis] Le retour au papier permet à deux hôpitaux d'assurer la continuité des soins suite à une attaque par rançongiciel. [>>Lire l'article](#)

Le 20 avril 2022, deux hôpitaux américains de Palm Beach, en Floride, ont essuyé une attaque par rançongiciel. Le soir même, les systèmes informatiques et lignes téléphoniques ont pu être rétablis dans les établissements visés.

CYBERVEILLE SANTE, 04/05/2022

Cybersécurité : focus sur les actions menées auprès des établissements de santé et structures médico-sociales en Auvergne-Rhône-Alpes. [>>Lire l'article](#)

En 2021, l'ARS Auvergne-Rhône-Alpes a recensé 60 signalements de cyberincidents visant des structures de santé ou médico-sociales, contre 55 en 2020. La recrudescence des actes cybermalveillants se vérifie également au niveau national, avec plus de 730 déclarations d'incidents en 2021, contre 369 en 2020.

DSIH, 09/05/2022

ANSSI : Rapport d'activité 2021.

[>>Lire l'article](#)

L'agence a déployé des parcours de cybersécurité pour les collectivités territoriales, les hôpitaux et les établissements public.

ANSSI, 11/05/2022

BONNES PRATIQUES



5 caractéristiques essentielles pour une sécurité efficace des endpoints. [>>Lire l'article](#)

1. Une approche proactive des nouvelles menaces
2. Atténuation automatique sans intervention humaine
3. Flexibilité multi-site et multi-administrateur
4. Comblent les lacunes grâce au déploiement automatique
5. Visibilité

SOLUTIONS NUMERIQUES, 02/05/2022

ISO 27035, l'autre norme pour la gestion des incidents de sécurité informatique. [>>Lire l'article](#)

La maîtrise des concepts dans le monde des incidents de l'informatique, implique de suivre un certain nombre de normes et de règles, les outils peuvent parfois changer, mais le fond a le mérite d'exister et de rester dans toutes les normes.

PUBLI NEWS, 04/05/2022

L'assurance Cyber : à quoi peut-elle servir ? [>>Lire l'article](#)

Alors que les grandes entreprises se posent désormais la question de contracter une assurance pour leurs risques cyber, les ETI n'ont pas les mêmes possibilités de trouver des solutions alternatives. D'autant que la RC pro des dirigeants d'entreprise ne couvre plus la cyber.

GLOBAL SECURITY MAG, 19/05/2022

MENACES



Rapport des menaces 1er trimestre 2022 : le cyber conflit Ukraine- Russie domine le paysage. [>>Lire l'article](#)

Les experts d'Avast font état d'activités cybercriminelles en partie en baisse en raison du conflit armé, de la baisse continue des rançongiciels en circulation et de la hausse du nombre de botnets Emotet. Ils ont également mis au jour l'un des plus grands réseaux botnet-as-a-service du monde.

UNDERNEWS, 05/05/2022

La grande fuite de données » : vos informations personnelles partagées des centaines de fois par jour. [>>Lire l'article](#)

Un rapport d'une ONG irlandaise met en lumière l'étendue des données partagées dans le cadre des enchères publicitaires en temps réel, qui traquent votre comportement en ligne pour vous servir de la réclame ciblée. Des chiffres qui donnent le tournis.

01NET, 17/05/2022

VULNÉRABILITÉ



Vulnérabilités dans Google Chrome.

[>>Lire l'article](#)

Bulletin d'alerte du CERT Santé concernant trois types de failles dans Google Chrome.

CERT SANTE, 13/05/2022

Vulnérabilités dans Mozilla

[>>Lire l'article](#)

Bulletin d'alerte du CERT Santé concernant des vulnérabilités dans Mozilla.

CERT SANTE, 23/05/2022

Vulnérabilité dans le noyau Linux

[>>Lire l'article](#)

Bulletin d'alerte de CERT Santé concernant une vulnérabilité dans le noyau Linux.

CERT SANTE, 23/05/2022

RGPD/ JURIDIQUE



RGPD et PIA : deux sanctions européennes précisent les erreurs à éviter lors de l'analyse de l'impact sur la vie privée.

[>>Lire l'article](#)

RGPD et PIA : deux sanctions européennes précisent les erreurs à éviter lors de l'analyse de l'impact sur la vie privée.

- L'analyse d'impact ne peut se contenter de réponses « Oui / Non »
- L'analyse d'impact doit porter sur l'ensemble des risques du traitement et être réalisée avant le début du traitement

SOLEGAL AVOCATS, 01/05/2022

Ces grossières erreurs dans la gestion des mots de passe qui mènent au tribunal.

[>>Lire l'article](#)

On sait qu'une mauvaise gestion des mots peut représenter une porte d'entrée tentante pour les hackers malveillants. Cela peut être également, comme l'illustre cette affaire judiciaire, la source d'importants conflits internes.

ZDNET, 13/05/2022

Cookie walls : la CNIL publie des premiers critères d'évaluation.

[>>Lire l'article](#)

Depuis plusieurs mois, certains sites web et applications mobiles utilisent des « murs de traceurs » (« cookie walls » en anglais). Régulièrement interrogée sur le sujet et saisie de nombreuses plaintes, la CNIL publie des premiers critères permettant d'évaluer la légalité d'une telle pratique.

CNIL, MAJ du 29/03/2022

TRUCS ET ASTUCES



Retour sur la conférence en ligne : « Spam, phishing : comment les détecter et protéger votre boîte mail ? »

[>>Lire l'article](#)

Cybermalveillance.gouv.fr, AFCDP et Signal Spam ont participé à une conférence en ligne diffusée en direct le 11 mai 2022 pour expliquer aux internautes comment identifier et signaler les messages de spam et de phishing, les risques et conséquences possibles de ce type de messages, et les bonnes pratiques à adopter pour s'en protéger.

CYBERMALVEILLANCE, 17/05/2022