15/03/2023

Reciproc-it

SYMBIOSE DE L'ENSEMBLE DES ACTEURS DE LA SANTÉ ET LE DÉFI SÉCURITÉ

Le bilan 2022 du 10ème congrès national de la sécurité des systèmes d'information dans le secteur de la santé a été marqué par trois jours de discussions réunissant 220 professionnels. Une forte présence des RSSI, DPO et DSI, une population concernée et inquiète de l'ampleur de la menace. Trois jours denses, d'échanges sur la situation en 2022 et les prochaines mesures à mettre en place, un nouveau référentiel en construction MaturiN'H, les alertes de l'ANSSI...

⚠ Les **hôpitaux** représentent la **troisième cible** des groupes cybercriminels, derrière les TPE, PME, ETI et les collectivités territoriales (rapport de l'ANSSI).

Les conséquences constatées :

- **Fuite de données confidentielles**: les informations que vous détenez sur les patients tels que les antécédents médicaux, les résultats d'examens, les informations de contacts sont des données sensibles : elles peuvent être utilisées à des fins malveillantes.
- **Réputation entachée**: vous perdrez la confiance de vos patients et de vos pairs.
- **Responsabilité juridique**: en vertu de la loi sur la protection de la vie privée, vous êtes responsables des données que vous possédez et pourriez être poursuivis en justice en cas de violation de cette obligation.
- **Coûts financiers**: les coûts associés à la récupération des données et à la restauration des systèmes informatiques peuvent être considérables.

Le dispositif **Ségur du numérique en santé** a pour objectif de généraliser le **partage** et la **numérisation** des informations de santé entre professionnels et usagers tout en garantissant la **protection** des données de santé.

Aujourd'hui, le grand défi est de sécuriser un système d'information complexe en digitalisation continue.
Nous nous positionnons dans cet écosystème pour **accompagner** dans la sécurisation de ces parcours.

Notre solution d'analyse de risques labellisée par **l'ANSSI**, **Oligo Risk Manager**, vous accompagne pour **identifier et maîtriser** ces risques et ainsi être en **conformité** avec les référentiels en vigueur.

Oligo • RM

- **Identifiez** vos **risques potentiels** et **prenez des mesures** pour renforcer la sécurité de vos systèmes d'informations.
- Évitez des **coûts financiers** considérables grâce à la prévention des attaques.
- Améliorez votre **réputation** auprès des patients et de l'écosystème médical.
- Prenez des **décisions éclairées** en matière de cybersécurité, en fournissant une vue d'ensemble des risques potentiels et des mesures à prendre pour les prévenir.
- Renforcez votre résilience face aux cybermenaces.

Vous êtes intéressés ? Contactez-nous dès maintenant pour une démo.

Je veux une démo!

L'actu de ce début d'année

Banque Centrale Européenne : un test de cyber-résilience pour 2024

En collaboration avec les autorités nationales, l'objectif de ce test sera d'évaluer la capacité des banques à maintenir leurs activités critiques en cas d'incident majeur.

Chat GPT : attention au partage de données confidentielles !

Malgré l'aspect révolutionnaire de cette IA, Chat GPT n'est pas un rempart face aux cybermenaces.

Les données transmises à cet outil sont susceptibles d'être volées au même titre que des données transmises via des mails ou des SMS. Des grandes entreprises américaines telles que Amazon ou JP Morgan ont déjà pris des mesures afin d'alerter et de restreindre l'usage de Chat GPT.

Ukraine-Russie: le premier aperçu d'une cyberguerre

En plus des combats sur le terrain, il existe bel et bien une guerre numérique qui se déroule dans l'ombre.

Depuis le début du conflit, russes et ukrainiens mènent des campagnes de désinformation et des actions de piratages en tout genre sur leurs infrastructures sensibles.
Le soutien de nombreuses entreprises du numérique telles que Microsoft et Google et l'anticipation de la menace ont contribué à la résistance de l'Ukraine face à ces cyberattaques.

Paypal: soupçons de non-conformité à la FTC et au NIST

Ce sont 35 000 personnes qui ont été touchées après un incident de sécurité survenu à la fin de l'année 2022.

D'une part, les plaignants accusent Paypal de ne pas être conforme aux directives de la FTC en affirmant que l'entreprise a été négligente dans la protection des données de ses utilisateurs. D'autre part, il semblerait que Paypal ne soit pas en conformité avec le référentiel NIST qui permet d'établir les bonnes pratiques en matière de cybersécurité.

Reciproc-it