STAGE 1ere année de Célia Baylet :

OKANTIS

1ère semaine du 27 mai au 31 mai 2024

27/05/2024

-J'ai commencé par la lecture et signature de la charte informatique, comme tout nouvel arrivant à Okantis.

-Il m'est attribué un compte personnel permettant l'accès aux ressources et ainsi qu'une adresse email de l'entreprise.

-Cet après-midi j'ai assisté à une réunion de sensibilisation pour tout nouvel arrivant à Okantis, sur la sécurité du système d'information (SI) : rappel des critères de DIC (disponibilité, intégrité, confidentialité) + preuve des données. On doit protéger les données sensibles des menaces et vulnérabilités, en mettant en place des mesures de sécurité. Rappel des bons usages; verrouiller le poste informatique, utiliser un système d'authentification à double facteur, longueur des mots de passe, faire attention au phishing… J'ai découvert le filtre de confidentialité sur les ordinateurs portables, qui peut être utile en déplacements notamment.

28/05/2024

-Aujourd'hui j'ai lu le référentiel de certification HDS de 2023 (68pages). J'ai appris qu'une certification dure 3 ans, et doit être évaluée tous les ans.
-On m'a parlé du site "Legifrance" pour rechercher ce type de document (car un référentiel peut être opposable.

29/05/2024

-Ce matin sur un fichier Excel j'ai noté les numéros, les noms des chapitres et les exigences requises du référentiel de certification HDS, pour un audit.

-Cet après-midi, j'ai repris ce référentiel pour faire un document avec le vocabulaire et les acronymes que je ne connaissais pas. Il y a beaucoup d'acronymes dans ce domaine. (voir annexe 1)

-J'ai participé à une réunion de l'équipe sécurité.

-J’ai commencé la lecture de la Politique de Sécurité des Systèmes d’Information (PSSI) d’Okantis (version 3.4).

30/05/2024

Dans les 2 semaines à venir je vais faire un audit d'une application web "lynksee", qui est encore en développement. Pour voir les éventuelles failles auxquelles les développeurs n'auraient peut-être pas pensé.
J'ai commencé par lire le "Guide d’utilisation : Formulaire du test d’intrusion". Le guide utilisation de l'ANS (l'Agence du Numérique en Santé) porté sur le test intrusion (méthode d'évaluation de la sécurité d'un SI (système d'information)). J'avais commencé à lire une version puis j'ai lu une version plus récente, c'est intéressant car nous pouvons voir les modifications effectuer comme par exemple : avec la version7 à partir de 3 gravités "moyenne" l'application ne pouvait pas être référencé, maintenant avec la version 15 c'est à partir de 10, cela laisse une plus grande marge. Les gravités sont soit classée "Moyenne", "Haute" ou "Non Applicable". Pour une gravité classée "Haute" à partir d’une seule c’est tout de suite éliminatoire, donc ne peut pas être référencé. Dans le cas d’une gravité classé "Non Applicable", dans le cas ici d’une application web, cela ne pose pas de problème.

(voir annexe 2)

J'ai regardé comment a été fait le document Excel, qui sera à remplir par la suite, il est appelé "cadre de réponse".

Ensuite il faut se demander "de quoi ai-je besoin pour réaliser l'audit technique ?", bien sûr de l'application web. Pour faire des tests sécurisés, nous pouvons avoir besoin d'une kali linux.

Ils m’ont dit que l’on pouvait installer kali directement sur notre ordinateur avec "microsoft store".

Normalement pour les machines virtuelles, ils utilisent ware workstation player. J'ai installé la dernière version de Virtual Box pour Windows. Ensuite je suis allée chercher l'image (ISO) kali sur leur site : https://www.kali.org/get-kali/#kali-installer-images

Nom de la kali : 'AuditAppWeb'

J'ai appris le terme de "Partitionner le disque" : consiste pour un système d'exploitation à le diviser en zones distinctes, dans lesquelles il va

pouvoir gérer les données et les informations de manière séparée et privée.

Logiciel d'amorçage (GRUB), c'est un noyau linux. Donc je l'ai installé sur le disque.

On m'a transmis un lien, pour avoir accès à l'application. Pour le transfert du mot de passe, je l'ai reçu via "locktransphobe".

J'ai téléchargé "Nodepad++", pour modifier la table host. Il est nécessaire lorsque l'on est connecté sur le réseau interne, de modifier sa table host pour se connecter à l'environnement de test.

Le chemin racine du fichier est celui-ci :
C:\Windows\System32\drivers\etc\hosts

31/05/2024

-Ce matin : relecture du tableur Excel pour être sûr de bien tout comprendre, j'ai recherché du vocabulaire. (voir annexe 3)

-Sur le site de la CNIL, j'ai recherché "Qu'est-ce ce qu'une donnée de santé ?" (voir annexe 4)

Annexe 1

Référentiel de certification Hébergeur de données de santé (HDS) 2023

Vocabulaire :

pages 6-8 définitions

referentiel : Système de référence (Action ou moyen de se référer, de situer par rapport à.)

Réversibilité : Caractère de ce qui est réversible. (Qui peut se reproduire en sens inverse.)

Mandater : Investir d'un mandat. (acte par lequel 1 personne donne à une autre le pouvoir de faire qqc en son nom)

Accréditation : Fait d'accréditer, de donner à (qqn) l'autorité nécessaire pour agir en qualité de ; fait d'être accrédité.

accrédité : Rendre quelque chose croyable, vraisemblable ou reconnaître officiellement comme vrai en parlant de quelqu'un, d'un organisme.

(Article) susvisé : Visé plus haut.

Intrinsèque : Qui est intérieur et propre à ce dont il s'agit.

Consubstantiel : Qui est unique par la substance. // inséparable de

Sujétion : Situation d'une personne soumise à une autorité souveraine ou astreinte à une nécessité ; obligation pénible, contrainte.

Portabilité des données : permet à la personne concernée d'obtenir ses données à caractère personnel et de les réutiliser pour d'autres services.

Matrice de correspondance : instrument qui montre les unités communes de résultats d'apprentissage entre différents pays pour une qualification donnée

Non-répudiation : consiste en l'assurance qu'une action sur la donnée réalisée au nom d'un utilisateur (après authentification) ne saurait être répudiée (Rejeter, repousser) par ce dernier.

l'impartialité / être impartial : Qualité, caractère de quelqu'un qui n'a aucun parti pris ou de ce qui est juste, équitable

gouvernance : un ensemble de décisions, de règles et de pratiques visant à assurer le fonctionnement optimal d'une organisation,

accords multilatéraux (de reconnaissance internationaux): multilatéral = Qui concerne plusieurs parties contractantes

perimetre de la certification : il s'agit de connaitre les activités qui sont incluses dans le Système du Management de la Qualité

SecNumCloud : permet aux utilisateurs finaux d'identifier des offres cloud qui visent en particulier à protéger les données et les traitements sensibles face à la menace cybercriminelle et à l'application de lois extraterritoriales.

Acronymes :

CSP : Code de la santé publique

DSCP :Données de Santé à Caractère Personnel

HDS: Hébergeur de Données de Santé

RGPD :Règlement Général sur la Protection des Données

SMSI :Système de Management de la Sécurité de l’Information

COFRAC : Comité Français d’Accréditation

DdA : Déclaration d’Applicabilité documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées et applicables au Système de Management de la Sécurité de l’Information d'un organisme

HDS : Hébergeur de Données de Santé

IAF :International Accreditation Forum

CEI / IEC : Commission Electrotechnique Internationale / International Electronical Commission

ISO :International Organization for Standardization

OC : Organisme de Certification

Annexe 2

Vocabulaire :

--Le jeton CSRF est une protection qui requiert l'insertion d'une valeur aléatoire et dynamique dans une requête. Cette valeur est ensuite analysée par le serveur pour déterminer si la requête est légitime.

-TSP : Un TSP (Technology Service Provider) est l'évolution et surtout l'innovation des services TI pour votre entreprise. Contacter un TSP, c'est contacter un expert prêt à répondre à tous vos besoins TI. Il est axé sur la gouvernance technologique et la transformation numérique de toutes vos exigences.

TI : TI (technologie de l'information) désigne le terme générique qui englobe les technologies qui facilitent le traitement de l'information. Les TI peuvent inclure les logiciels, le matériel, les ressources réseau, les technologies de communication et les autres services associés.

Annexe 3

VOCABULAIRE :

Comptes génériques : sont souvent attribués à des partenaires, intervenants externes ou limités dans le temps

CVSS : Common Vulnerability Scoring System est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.

HTTP Strict Transport Security : HSTS : permet à un site web d'informer le navigateur que son accès ne devrait pas se faire en HTTP et qu'il devrait donc convertir toute tentative de connexion en HTTP en connexion HTTPS

Encodage : Processus de production d'un message selon un code.

L’assainissement de données : vise à améliorer la qualité des données qui est définie selon des paramètres d’exactitude, d’exhaustivité et d’unicité

secure attribute : Seul l’attribut secure vous permettra d’empêcher qu’un Cookie ne soit jamais communiqué en HTTP simple.

CSRF : (Cross-Site Request Forgery) est une attaque qui usurpe l'identité d'un utilisateur de confiance et envoie des commandes non désirées sur un site web.

La méthode HTTP TRACE est une méthode souvent utilisée pour le débogage ou la recherche d'information.

Le débogage : est le processus qui consister à trouver et à corriger les erreurs ou les bogues dans le code source d'un logiciel.

XML external entity attack : L'attaque d'entité externe XML, ou simplement l'attaque XXE, est un type d'attaque contre une application qui analyse l'entrée XML. Cette attaque se produit lorsqu'une entrée XML contenant une référence à une entité externe est traitée par un analyseur XML faiblement configuré.

L'en-tête Content-Type: sert à indiquer le type MIME de la ressource. Dans les réponses, un en-tête Content-Type indique au client le type de contenu réellement renvoyé. Le fait d'indiquer le type MIME de chaque ressource permet au navigateur de l'utilisateur de récupérer des contenus correctement identifiés, et de fermer la porte à l'envoi de certains contenus dangereux.

HttpOnly : Protection contre le vol dans le navigateur.

Un réseau de diffusion de contenu (CDN) : est un réseau de serveurs interconnectés qui accélère le chargement des pages Web pour les

applications à forte densité de données. CDN peut signifier content delivery network ou content distribution network.

Html integrity : L'intégrité de domaine fait référence à l'ensemble des processus qui garantissent l'exactitude des données rattachées à un domaine.

Un Web Application Firewall (WAF) : protège le serveur d'applications Web dans le backend des multiples attaques (phishing, ransomware, attaque DDOS, malware). La fonction du WAF est de garantir la sécurité du serveur Web en analysant les paquets de requête HTTP / HTTPS et les modèles de trafic.

À chaque type de documents, on procède à une déclaration de type de documents (la DTD). Avoir une DTD permet ainsi de formaliser le squelette de n'importe quel fichier. Elle est externe si le document contient seulement une référence vers un autre document contenant la DTD.

Le dossier médical partagé : DMP

Annexe 4

Site de la CNIL : " Qu'est-ce ce qu'une donnée de santé ? "

Le règlement européen sur la protection des données personnelles (RGPD), qui est entré en application le 25 mai 2018, procède à une définition large des données de santé.
Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique
les informations relatives à une personne physique (un numéro pour l'identifier a des fins de santé)
les informations obtenues lors du test ou de l'examen d'une partie du corps (données génétique, échantillons biologiques)
les informations concernant une maladie (handicap, risque de maladie, antécédent, traitement)
Cette définition permet d'englober **certaines données de mesure à partir desquelles il est possible de déduire une information** sur l'état de santé de la personne.
deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques…), croisement de la tension avec la

mesure de l’effort, etc. Mais pas seulement une application de compteur de pas car aucune conséquence peut en être tiré.

Une fois la qualification de données de santé retenue, un régime juridique particulier justifié par la sensibilité des données s’applique. Par exemple :

- loi Informatique et Libertés ;
- dispositions sur le secret ;
- dispositions sur l’hébergement des données de santé ;

Rappel : CSP = Code de la Santé Publique

Les données de santé sont des données à caractère personnel particulières car considérées comme sensibles, afin de garantir le respect de la vie privée des personnes.

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable.

- directement (nom, prénom) ;
- indirectement (numéro de téléphone, plaque d’immatriculation, identifiant tel que le numéro de sécurité sociale, adresse postale ou courriel, la voix, l’image).