e-santé Occitanie
Connecter pour mieux soigner

HDS

Le label nécessaire mais pas suffisant

Bruno POUJOULAT 09/11/2021

SOMMAIRE

Que représente la certification HDS ?

- Historique
- Agrément vs certification
- Procédure d'obtention
- Les différentes certifications

De quoi cela ne vous exempte pas ?

- Ce qui reste de votre ressort
- Ce qui doit être clarifié

Qui doit y avoir recours ?

- Pour quelles activités ?
- Dans quelles situations ?
- Qui en est exempté ?

01

HDS, qu’est-ce que c’est ?

Hébergeur de données de santé

- Pourquoi légiférer ?
  - *« le législateur souhaite garantir la confiance dans les tiers auxquels des structures [...] confient les données de santé qu'ils produisent ou recueillent [...] au travers des critères de sécurité à l'état de l'art »*

FAQ HDS_16052019_V0 18.pdf (esante.gouv.fr)

- Historiquement un agrément, aujourd'hui une certification
  - Le décret du 4 janvier 2006 définissait la procédure d'agrément des hébergeurs de données de santé à caractère personnel.
  - Depuis le 1er avril 2018, l'agrément a été remplacé par une certification

- La différence d'obtention
  - Du déclaratif
  - À la preuve

Hébergeur de données de santé

Les différentes certifications

Il y a deux certifications pour 2 métiers distincts, qui regroupent 6 activités

- Certificat « hébergeur d'infrastructure physique »
  - mise à disposition et maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
  - mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.

- Certificat « hébergeur infogéreur »
  - mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
  - mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
  - administration et exploitation du système d'information contenant les données de santé ;
  - sauvegarde externalisée de données de santé.

Qui doit y avoir recours ?

Certification HDS: Quand ? Pour qui ?

Quand parle-t-on d'hébergement de données de santé ?

- L'article L.1111-8 du code de la santé publique indique que : « Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet ».

Quand doit-on y avoir recours ?

- Le Ministère des Solidarités et de la Santé précise que les personnes physiques ou morales tenues de recourir à un hébergeur agréé ou certifié sont d'une part, les patients qui confient l'hébergement de leurs données de santé à un tiers, et d'autre part les responsables de traitements de données de santé à caractère personnel ayant pour finalité la prévention, la prise en charge sanitaire (soins et diagnostic) ou la prise en charge sociale et médico-sociale de personnes

Certification HDS: Qui en est dispensé ?

- Qui en est exclu ?

  - […] ne constitue pas une activité d'hébergement au sens de l'article L. 1111-8, le fait de se voir confier des données pour une courte période […]
  - Un établissement n'a pas à être certifié HDS pour l'hébergement des données des patients qu'il prend en charge. Le certificat HDS étant relatif à l'entité légale, i.e. au n° SIREN, des établissements regroupés sous le même SIREN mais ayant des SIRET différents n'ont pas non plus l'obligation de certification.

- Quels sont les acteurs qui doivent être certifiés au titre de l'activité 5

  - […] le ministère chargé de la Santé va engager des travaux pour étudier l'opportunité et les modalités d'encadrement de l'activité d'administration et d'exploitation d'applications. Ces travaux pourront déboucher sur la mise en place d'un dispositif spécifique pour encadrer au mieux l'activité […]. Une modification du décret HDS pourrait être nécessaire pour préciser l'encadrement de l' «activité d'administration et d'exploitation des SI de santé»

De quoi cela ne vous exempte pas ?

Que reste-t-il sous votre responsabilité ?

- Tout ce qui n'a pas été contractualisé avec l'HDS et qui se rapporte au traitement des données de santé

  Potentiellement certaines activités parmi:

  - Sensibilisation des personnes
  - Gestion des habilitations
  - Maitrise des fournisseurs et sous-traitants
  - Respect de la finalité des traitements
  - Information sur la collecte
  - Gestion et protection des actifs
  - Acquittement des échanges
  - Protection des échanges sur les réseaux publics/privés
  - Définition, protection et validité des sauvegardes
  - Définition des besoins de PCA/PRA
  - Etc.
  - Mais surtout respecter la PGSSI-S

Et encore

- Il est du ressort de chaque ES d'identifier toutes les lois et réglementations auxquels il est soumis. Ainsi des établissements publics peuvent voir leurs archives classées comme « archives nationales ». Et l'hébergement des archives nationales peut présenter des exigences propres, comme l'hébergement exclusif sur le territoire français.

- La certification HDS impose à l'hébergeur de « *proposer* » à ces clients le pays d'hébergement mais il n'y a pas de restrictions/obligation concernant lesdits pays. Seule la langue française est, à minima, obligatoire dans la documentation

Merci de votre attention.

e-santé Occitanie
Connecter pour mieux soigner

Thématique:

Gestion des sauvegardes et restaurations

E-Santé Occitanie

Mardi 9 NOV 2021

Pascale RANGER
09/11/2021

RésO
La solidarité en mouvement

Gestion des sauvegardes et restaurations
Agenda de la réunion

FONDAMENTAUX ET BONNES PRATIQUES

RETOUR D'EXPÉRIENCE

QUESTIONS, ECHANGES, RESSOURCES

Fondamentaux et bonnes pratiques

LES 4 PILIERS DE LA SÉCURITÉ INFORMATIQUE ET DE LA PROTECTION DES DONNÉES

Intégrité

Fiabilité et crédibilité des données durant tout leur cycle de vie

Confidentialité

Seules les personnes autorisées accèdent aux données

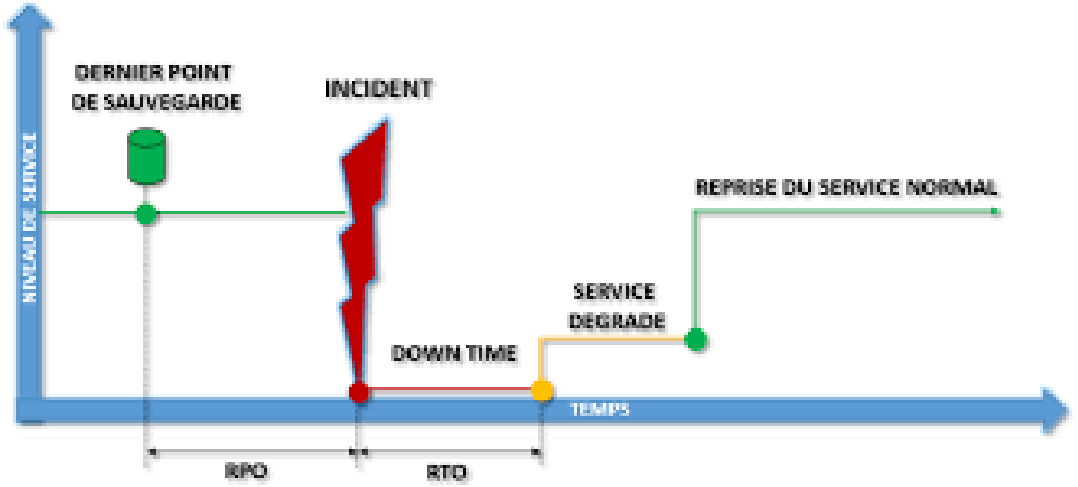
Disponibilité

Accessibilité aux données pour les utilisateurs

Preuves

Savoir qui a accédé à quelles données et quand pour analyser une situation

FOCUS SUR LA PERTE D'INTÉGRITÉ ET DE DISPONIBILITÉ DES DONNÉES LORS D'UN INCIDENT



RPO : Recovery Point Objective

Perte de données maximale admissible (perte d'intégrité)

RTO : Recovery Time Objective

Durée maximale d'interruption admissible (perte de disponibilité)

PCA ET PRA

PCA Plan de Continuité d'Activité

« comment on continue l'activité malgré une grève, un attentat, un incendie, un crash informatique… » (Plan Bleu, Plan Blanc)

⇒ Cas où la continuité de l'Activité de l'organisation est assurée ou non

⇒ Organisation et procédures dégradées selon ces cas

⇒ Besoins minimums et priorité de la Direction et des métiers sur

- ⇒ sur la sécurité des données (disponibilité, intégrité, confidentialité, preuves)
- ⇒ sur les moyens informatiques / papiers pour ces données

PRA Plan de Reprise d'Activité

« comment on rétablit l'activité en mode standard »

⇒ Moyens mis en œuvre pour remonter le système d'information en tenant compte des priorités

LA SAUVEGARDE

Définition	Opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système d'information. Les données sont dites « à froid » (déconnectées de la production) On sauvegarde des données à plat, des bases de données ou des VM (machines virtuelles)
Usage	Assure l'intégrité des données C'est indispensable Répond au PRA
Atouts	Stockage moins performant et moins cher Granularité possible Couvre tous les cas / scénarios de menace

CONCEPTS CLÉS AUTOUR DE LA SAUVEGARDE

- ✓ Sauvegarde totale
- ✓ Fréquence de sauvegarde = Toutes les heures, tous les jours (~RPO)
- ✓ Sauvegarde incrémentale = Sauvegarde du différentiel des données avec la sauvegarde totale
- ✓ Sauvegarde full synthétique = Reconstruction d'une sauvegarde utilisable somme de la sauvegarde totale et de la sauvegarde incrémentale
- ✓ Rétention = Durée de conservation de la sauvegarde
- ✓ Plan de sauvegarde = Document qui définit les types de sauvegardes, la fréquence, l'espace et le lieu de stockage, la rétention)

COMMENT JE RESTAURE À PARTIR DE MA SAUVEGARDE ?

	Cas 1: restaurer une/des données à plat	Cas 2: restaurer une image du système complet	Cas 3: réinstaller le système, les applications et restaurer une base de données
Moyen	Microsoft a intégré des sauvegardes automatiques Cette restauration peut être réalisée par l'utilisateur lui-même en toute autonomie	On va chercher l'image de la veille ou des jours précédents de la machine virtuelle avec le système, les données à plat et les bases de données	Repartir d'une VM nue, réinstaller l'OS, déposer la dernière sauvegarde valide des données à plat et des bases de données Faire réinstaller l'application par l'éditeur

BONNES PRATIQUES LIÉES À LA SAUVEGARDE ET À LA RESTAURATION

- Définir les besoins et obligations règlementaires avec les métiers
- Communiquer la stratégie de sauvegarde aux utilisateurs
- Externaliser les sauvegardes
- Contrôler & relancer les sauvegardes qui échouent
- Faire régulièrement des tests de récupération de données, des bases de données et de restauration des VM
- Avertir les référents métiers / direction quand un risque d'intégrité (sauvegarde échouée, restauration non fonctionnelle) est avéré
- Tester le PRA

LA RÉPLICATION DE DONNÉES

Définition	Redondance en actif-actif ou en actif-passif des données et des applications sur 2 Datacenters. Les données sont dites « à chaud » (données de production) Système à tolérance de panne = il peut y avoir une panne, c'est transparent pour les utilisateurs
Usage	Améliore la disponibilité des données C'est un plus pour répondre à un PCA **La réplication de données ne remplace pas la sauvegarde**
Atouts	Permet de repartir beaucoup plus vite Améliore les performances grâce à la répartition

RETOUR D'EXPÉRIENCE

RETOUR D'EXPÉRIENCE D'UNE CYBERATTAQUE CHEZ RESO

RESO: Association Résilience Occitanie

- Structure Médico sociale
- 35 établissements et services implantés
- 3 départements (Haute Garonne, Tarn et Garonne, Ariège)
- 1100 salariés
- 2400 usagers (enfants, adolescents, adultes, majeurs protégés, personnes âgées)

Retour d'expérience sur attaque via crypto-virus mi-août 2021

- ✓ Contexte de l'informatique chez RESO
- ✓ Stratégie de reconstruction
- ✓ De l'utilité des sauvegardes

CONTEXTE DE L'INFORMATIQUE CHEZ RESO AVANT ATTAQUE

Forces et Opportunités

- SI hébergé chez Hébergeur infogérant toulousain Fullsave <u>depuis avril 2020</u>
  - *~40 VM & 5To de données sauvegardées quotidiennement avec Veeam sur rétention de 15 jours*
    - *Données*
    - *Bases de données*
    - *Profils utilisateurs des bureaux virtuels*
    - *VM*
  - *Réplication asynchrone des données avec Netapp toutes les heures entre 2 Datacenters*
- Service d'infogérance sur l'assistance aux utilisateurs, support niveau 1, intervention sur site <u>depuis mai 2021</u>
- Arrivée nouvelle RSI <u>depuis juin 2021</u>

Faiblesses et Menaces

- SI local restant sur certains sites
  - *Quelques anciens serveurs locaux, NAS ou ESXi non sauvegardés*
- Absence de formalisation des procédures
  - *Modes dégradés côté métier*
  - *PRA*
  - *Documentation technique et opérationnelle (architecture, config, install, plans de tests…)*
- Socle technique (AD, serveur de fichier, serveur d'impression, antivirus, bureaux citrix, messagerie) non infogéré et vulnérable (Obsolescence OS, gestion des comptes administrateurs)
- 40% de postes en windows 7

DÉROULEMENT ET ANALYSE FORENSIC DE LA CYBERATTAQUE DU 13/08/2021

- Carte d'identité du virus : ransomware Lockbit 2.0
- Matérialisation de l'incident de sécurité :
  - Des données sont retrouvées chiffrées .lockbit sur serveurs et postes de travail
  - Des ramettes de papier sont retrouvées imprimées « Lockbit » par les imprimantes
- Ce qui a été fait & impact :
  - Ouverture de l'incident auprès de l'ARS – soutien, conseil du CERT Santé
  - Ouverture de l'incident auprès de la CNIL
  - Déconnexion du réseau de chaque VM et isolation des sites
  - Service extrêmement dégradé avec juste possibilité de démarrer son pc en local: plus d'accès aux applications et données partagées
- Méthode de propagation :
  - L'attaquant a rapidement pu prendre possession des privilèges les plus élevés sur le Système d'Information (compte « Administrateur ») et notamment s'est créé un compte d'administrateur du domaine (compte « Luci »)
  - Ces deux comptes ont été utilisés dans le cadre du déploiement généralisé du ransomware
  - L'AD et tout le SI est compromis

ELÉMENTS QUI ONT PERMIS DE BÂTIR LA STRATÉGIE POUR REMONTER LE SI

- Possibilité de s'appuyer sur ses sauvegardes saines
- Activité réduite en été
- Volonté de ne pas payer de rançon
- Ne pas risquer de garder des traces du virus lors de la remontée du SI
- Rendre l'infrastructure conforme aux bonnes pratiques SI et SSI
- Profiter de la crise pour mettre en place en 3 mois « toute » la feuille de route infrastructure

Stratégie adoptée : Restauration des sauvegardes = Cas 3 (slide 9)

CRISE CYBER : ETAPES DU PLAN DE REPRISE INFORMATIQUE

- Création d'un nouveau socle technique (réseau, hyperviseur, sécurité, poste de travail virtuel RDS)
- Renforcement de la sécurité (aspect preuves) avec mise en place d'un nouveau FW Palo Alto
- Création d'un nouvel AD avec nouveau domaine
- Création de plusieurs VMs pour réinstallation des applications
- Contrôle d'intégrité sur les bases de données et données applicatives (2 filtrages anti-virus distincts)

(restauration du 13/08 ou du 12/08 voire du 09/08)

- Mise à disposition des données et bases de données sur les serveurs applicatifs
- Réinstallation des applications par les éditeurs, puis des interfaces applicatives
- Validation des remontées applicatives par les référents métiers
- Réinstallation de tous les postes de travail avec nouveau master et inventaire
- Externalisation de la messagerie sur Microsoft O365
- Formalisation de la documentation process IT, technique et opérationnelle au fur et à mesure

CRISE CYBER : NIVEAU DE SERVICE DU SI AU REGARD DES 4 PILIERS DE LA SÉCURITÉ

Intégrité

Perte de données 1 à 5j en DC. 4% de pertes de données (chiffrées) sur les sites (non sauvegardé)

Confidentialité

Pas de vol de données constaté ni revendiqué

Disponibilité

De 1 semaine à 3 mois pour remonter les applications et redonner les accès aux utilisateurs

Preuves

Logs existants mais parfois insuffisants pour valider le vecteur d'intrusion et patient 0

Questions et Echanges

QUESTIONS, ECHANGES

Archivage & Données Personnelles

- Direction des Archives Départementales : Obligations règlementaires de conservation de données pour archivage sur 10 ou 20 ans, visa
- Règlementation RGPD : un usager peut demander à supprimer ses données personnelles. Sauvegarde ok avec rétention de 1 mois. Archivage concerné également.

RESSOURCES

ANSSI – France Relance – Sauvegarde sécurisée
https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-sauvegarde_securisee.pdf

ANSSI – Bonnes pratiques de sécurité pour les TPE/PME
https://www.ssi.gouv.fr/uploads/2021/02/anssi-guide-tpe_pme.pdf

ANSSI – Liste des Prestataires de Détection des Incidents de Sécurité (PDIS)
https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/

ANSSI – Bonnes pratiques pour l'administration sécurisée des systèmes d'information
https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/

ANSSI – Guide d'hygiène informatique
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

RESSOURCES

Une méthodologie générale pour élaborer un plan de continuité de l'activité (PCA)
guide-pca-sgdsn-110613-normal.pdf

Guide de l'ANAP pour les GHT, plus axé informatique
pgssi-s_guide_pci_v1.0.pdf (esante.gouv.fr)

Ressources ANAP dans le cadre du programme HOP'EN
https://ressources.anap.fr/numerique/publication/2405
https://ressources.anap.fr/numerique/publication/2397-atteindre-les-prerequis-hop-en/6448-fiche%C2%A03-%E2%80%94-plan-de-reprise-d-activite-et-procedures-de-fonctionnement-en-mode-degrade