Cybersécurité.
Retour sur la cyber attaque de Dax
Et Comment sécuriser nos services de radiothérapie ?

Mardi 08 novembre 2022

Dr Nicolas PONTIER

CH de Dax

RADIOTHÉRAPIE - QUOI DE NEUF ?

ACTUALITÉS DES CONGRÈS SFRO ET ASTRO 2022

Liens d’intérêts

Aucun

Introduction

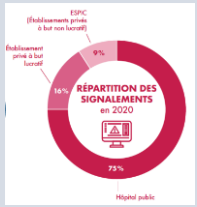
Structures de santé = secteurs à risque

Intégration du numérique depuis des décennies sans réelle démarche sécuritaire

Cyberattaques des établissements de santé

X2 entre 2020 et 2021 (730 en France en 2021)

Conséquences lourdes:



Déclenchement plan blanc

Déprogrammation des patients

Retard de prise en charge voire mise en danger des patients

Risque cyber parfois perçu comme secondaire par les professionnels de santé :

30% ne se sentent pas concernés par la cybersécurité[1]

[1] Enquête Eurogroup Consulting – Aout 2021: https://www.eurogroupconsulting.com/fr/2021/08/24/cybersecurite-dans-les-etablissements-de-sante/

5 facteurs de risque

4 facteurs« techniques »

- Multiplication des logiciels applicatifs
- Connexions peu sécurisées entre SI hospitaliers et SI des prestataires
- Connexion à internet des dispositifs médicaux en croissance
- Installation de logiciels sans l'approbation des services informatique

1 facteur humain

- Equipes peu sensibilisées aux menaces cyber, manque de connaissances

Ces fragilités **et l'essor des données de santé monnayables** encouragent les cyber attaques

Radiothérapie - Quoi de neuf ? (2022)

Les menaces?

4 ordres:

Le phishing

(Usurpation d'identité): **Le but est de voler des données**.

de nombreux sites d'organisations de santé sont imités:

SIDEP, Ameli pro, l'OMS, le CDC…

Vol de données

faiblesse des infrastructures + la « richesse des données de santé ».

Les hôpitaux gèrent des informations sensibles

Un dossier médical peut valoir **350 $** sur le marché noir :**50 fois plus qu'un dossier bancaire** [1]

L'Assistance publique-hôpitaux de Paris a été victime en 2020 du vol de données concernant 1,4 millions de personnes [2]

Attaques par déni de service (attaques DOS):

L'objectif est d'interrompre les communications d'une structure par un envoi massif de requêtes pour saturer les systèmes.

Certains hôpitaux ayant subi ce genre d'attaque ont dû transférer en urgence leur patients. (hôpital Tchèque en 2020).

Les ransomwares (dax)

Le but est l'extorsion d'argent.

Le système est paralysé en quelques minutes.

Les hackers pratiquent la « double extorsion » en proposant de délivrer les « clés » des données chiffrées (si la rançon est réglée), et menaçant par ailleurs d'exposer publiquement les informations. (Corbeil-Essonnes)

C'est la menace principale selon un rapport du gouvernement en 2020 [3]

[1] Enquête Eurogroup Consulting – Aout 2021: https://www.eurogroupconsulting.com/fr/2021/08/24/cybersecurite-dans-les-etablissements-de-sante/
[2] https://abonnes.hospimedia.fr/articles/20210916-systeme-d-information-l-ap-hp-porte-plainte
[3] [1] https://s3-eu-west-1.amazonaws.com/static.hospimedia.fr/documents/213895/6592/Rapport-activite-cybermalveillancegouvfr-2020.pdf?1618499514

Cyberattaque, Dax 2021 : les faits

Service : 2 accélérateurs /1 scanner, File active: 80 patients/j soit 850-900/an

9 février 2021 (02h)
Cyberattaque
ransomware (cryptovirus Ryuk)
Suspicion de « panne géante »

9 février 2021 (03h)
Arrêt total du SI hospitalier
Contamination de 150 serveurs (>85%)

Mise en alerte du SAMU
Et déprogrammation

Arrêt du service de radiothérapie pour une durée inconnue :
Décision urgente!

Premier temps
- Reprendre **au plus vite** les traitements des patients
- (avec le maximum de sécurité possible…)

deuxième temps
- **Adresser ailleurs** les patients prévus
- Appel à 5 structures entre Bayonne, Pau, Tarbes et Bordeaux 55-150 kms

Priorisation des patients

Ont été priorisés (fonction de la pathologie et de la curabilité) :
- **1** cancers curables avec tumeur en place
- **2** les patients métastatiques urgents
- **3** les cancers du sein en adjuvant et de prostate.

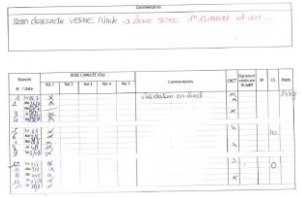
Adressage : fonction du domicile, de la capacité d'accueil, de la spécificité et réactivité des centres.

Radiothérapie - Quoi de neuf ? (2022)

Modalités de prise en charge

1- répertorier les patients

- Fiche papier de radiothérapie, **seul document accessible**
- Chaque patient a été contacté

2-Traitement à Dax

- **En mode service sur le clinac** (accord de l'ASN)
- patients avec traitements simples, facilement positionnables (sans MLC)
- avec triple vérification manip/physique/médecin)

3-Adressage des autres patients

dans les centres de la région : (Conventions)

- Envoi par fax les éléments de dossier disponibles
- Déplacement des radiothérapeutes et physiciens de Dax en renfort des équipes
- Nouveau scanner et délinéation
- Plan de traitement recalculés
- Comparaison aux éléments disponibles (fiche protocole, HDV)
- Pas de compensation des arrêts de traitements
- **Tout a été tracé**

Radiothérapie - Quoi de neuf ? (2022)

Patients prévus (non traités)

Ceux nécessitant une prise en charge avant fin Mars 2021 : ont été adressés semaine par semaine comme des « nouveaux patients » (délais à respecter, capacité d'accueil des centres et des avancées sur Dax).

Certains traitements **ont été reportés**

Radiothérapies antalgiques

traitement médical de la douleur et adressage uniquement si la douleur non contrôlable

Les cancers ORL évolués

l'option d'une chimiothérapie d'induction a été retenue (décaler de 6 à 9 sem. leur radiothérapie) :

Les cancers de prostate sous hormonothérapie

Les cancers du Sein sans chimiothérapie adjuvante

Radiothérapie - Quoi de neuf ? (2022)

Récupération, reprise d'activité

S6 Mars

- Réseau minimal en circuit fermé début mars 2021 (Varian)
- Récupération des données sur la sauvegarde de 3° niveau de l'hôpital (bandes magnétiques déconnectées)
- Récupération des données patients et accélérateurs **(6 sem.)**
- Contrôles qualités externes des 2 accélérateurs refaits à la demande de l'ASN

S8-11 mars_-Avril

- Reprise d'un premier accélérateur (True beam 31 mars 2021)
- Reprise du second accélérateur (Clinac 26 avril 2021)

S12 Mai

- Pleine charge du service fin Mai 2021 (circuit fermé)
- Reconnexion au SI hospitalier en Octobre 2021

Nous avons récupéré durant le printemps et le début de l'été 2021 les données des patients traités hors centre

Quasi aucune déviation n'a été constatée (1 séance oubliée pour un sein seul) **48Gy au lieu de 50**

Reconstruction du système

- **Sur des infrastructures informatiques neuves**
- **Réinstallation complète du SIH avec mot de passe renforcé**
- Aide de l'Agence nationale de la sécurité des systèmes d'information (Anssi) et d'Orange cyber défense.

Un Cloisonnement des serveurs a été effectué (serveurs « fusibles »)

Impact financier pour l'hôpital: 4 770 000 €

Investissements matériel	Prestations cybersécurité et réinstallations	Sous-traitance en biologie	Ressources humaines (renforts, heures sup etc…)	Pertes de recettes commerciales	Pertes de recettes (radiothérapie/ imagerie)
174 000 € (nouveaux serveurs)	**546 000€**	**9 000€**	**1 484 000€**	**143 000€**	**2 344 000 €**

(1,5% du budget du CH de Dax)

Radiothérapie - Quoi de neuf ? (2022)

Victimes privilégiées des attaques ?

62 % : la finance

25 % : les médias

8% : l'industrie, hôpitaux compris

5 % : les télécommunications

Les établissements de santé deviennent des cibles de plus en plus privilégiées.[1]
Les hôpitaux qui sont des secteurs « sensibles » nécessitent des protections renforcées en matière informatique

[1] : ANATOMIE D'UNE CYBER-ATTAQUE CONTRE UNE ENTREPRISE : COMPRENDRE ET PRÉVENIR LES ATTAQUES PAR DÉNI DE SERVICE.
« Annales des Mines - Gérer et comprendre » 2016/1 N° 123 | pages 5 à 14.
ISSN 0295-4397 DOI 10.3917 /geco1.123.0005. Article disponible en ligne à l'adresse :https://www.cairn.info/revue-gerer-et-comprendre-2016-1-page-5.htm

Radiothérapie - Quoi de neuf ? (2022)

Comment sécuriser nos structures ?

1 La stratégie principale reste préventive

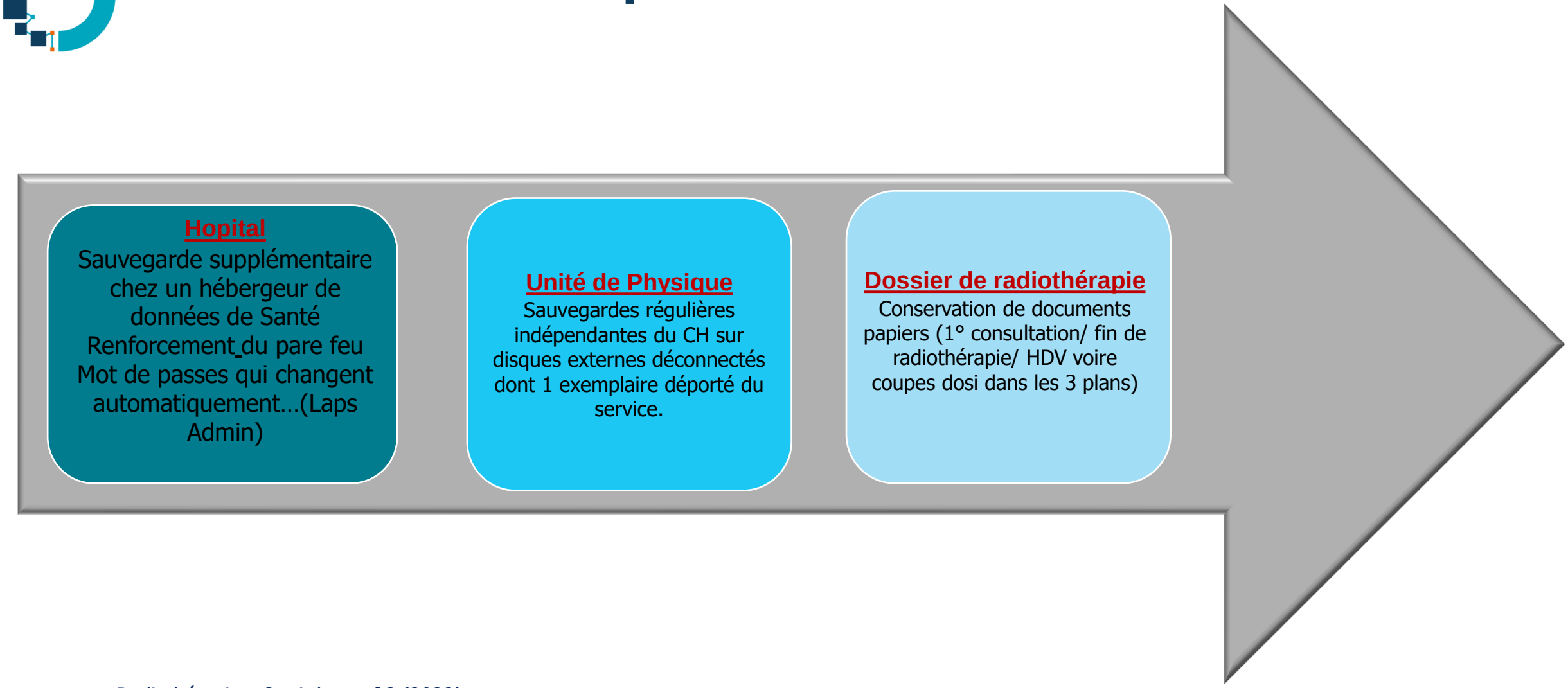
veille technologique, prévention des failles informatiques, sauvegardes régulièrement mises à jour (dont une si possible externalisée)

2 Audit externe : évaluer nos failles informatiques potentielles

3 Facteur humain…(collaboration avec les informaticiens)

4 Trouver un juste équilibre et protéger le site à hauteur des risques (protections coûteuses)

Actions mises en place à Dax



Actions au niveau gouvernemental

La stratégie ministérielle a été renforcée [1]

National

1 **Création d'un observatoire de « maturité informatique des établissements de santé »** (MaturiN-H).

2 **Création d'un Service national de cybersurveillance en santé**

Territorial

Pilotage par les ARS: **sensibilisation des acteurs**, (partage de pratiques) **mutualisation** des moyens et des capacités de réponse à incidents.

Structures de soins

Demande de **Prise en compte du risque cyber** dans la politique de maîtrise des risques de l'établissement à hauteur de **5 à 10%** du budget informatique

Contrôle

Sera Assuré Via l'HAS: **Certification prévue** qui devra Répondre aux exigences du Critère 3.06-02 : « risques numériques maîtrisés" »

Prévu que Les 891 hôpitaux français (135 GHT) soient intégrés à la liste des "**opérateurs de service essentiels**".

[1] https://esante.gouv.fr/sites/default/files/2022-01/DP-CYBERSECU-MONTE-201625-WEB.pdf

Généraliser les processus de gestion de crise

Rapidité de réaction: clé pour limiter ses conséquences

- Stratégie de gestion de crise cyber doit être construite par les DSI
- Définir un niveau de criticité des alertes (réponse adaptée à chaque situation).
- Constituer une cellule de crise
- Définir des plans de recours et de communication internes et externes: visent à réduire le temps de réaction et l'impact sur la prise en charge des patients selon des situations types définies.[1]

[1] Enquête Eurogroup Consulting – Aout 2021: https://www.eurogroupconsulting.com/fr/2021/08/24/cybersecurite-dans-les-etablissements-de-sante/

Conclusion

Les attaques informatiques des structures de santé sont en augmentation.

Derrière ces attaques il y a un objectif financier mais aussi parfois politique.

Les hackers identifiés proviennent de différentes régions du monde. certains faisceaux de preuves mènent régulièrement vers l'Europe de l'Est.

Il faut sécuriser nos failles, multiplier les moyens de sauvegardes afin d'être capable de reconstruire au plus vite notre système et minimiser les temps d'arrêt des traitements.

Le président de la République, a annoncé un plan d'1 milliard d'euros (350 millions issus du Ségur de la santé) pour renforcer la sécurité de nos systèmes.

•Un portail numérique unique existe pour les signalements d'incidents de sécurité : https://signalement.social-sante.gouv.fr/


MERCI
www.onco-nouvelle-aquitaine.fr