RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Auvergne-Rhône-Alpes

Gendarmerie nationale

GCS eSanté ARA la santé connectée

Collectif SI médico-social ARA

Webinaire de sensibilisation à la cybersécurité

Etablissements médico-sociaux

Jeudi 8 juillet 2021

Sommaire

1. Contexte & actualités
2. L'état de la menace cyber
3. L'organisation Gendarmerie & Police
4. La politique de prévention
5. Les réactions en cas d'attaque
6. Les RETEX

1. Contexte & actualités

Collectif SI médico-social ARA

- Le secteur de la santé connaît un **essor important du numérique** : soins, gestion administrative, etc. **La quasi-totalité des métiers de la santé et du médico-social sont concernés par le numérique.**

  L'omniprésence des données de santé s'est accrue avec la crise sanitaire.

- Depuis 2019 et 2020, **recrudescence des incidents SI et des actes de cyber malveillance** dans les secteurs sanitaire & médico-social.

- En 2020, 369 incidents ont été signalés au niveau national, dont 55 pour notre seule région. Hausse constante : en ARA, 32 incidents déclarés en 2018, puis 45 en 2019.

- Sous-déclaration probable : encore de nombreux incidents non-signalés.

Collectif SI médico-social ARA

- **Evolution du type d'incidents.** En 2018, au niveau national, 41% des incidents signalés étaient d'origine malveillante. Ce chiffre s'est établi à 60% en 2020.

- **Les établissements médico-sociaux, plutôt moins impactés il y a quelques années, sont de plus en concernés.**

- **C'est un signal d'alarme : le secteur médico-social est, aujourd'hui, moins préparé que le secteur sanitaire.**

- Dans ce contexte, il incombe aux établissements sanitaires & médico-sociaux de se protéger et de protéger leurs patients.

Les annonces gouvernementales

https://esante.gouv.fr/securite/cybersecurite

- Le 18 février, présentation de la stratégie Cyber par le Président de la République, déclinée en **plan de renforcement de la cybersécurité en santé en 2021** :

- Pilotage national au plus haut niveau du Ministère des Solidarités et de la Santé
- Appui national des structures par le CERT Santé renforcé
- Campagne nationale « Tous cyber vigilants » lancée le 9 juillet
- Investissements : plan de relance (136 millions d'euros pour renforcer l'Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI - et l'Agence du Numérique en Santé – ANS -), Ségur de la Santé (350 millions d'euros pour la cyber sécurité des secteurs sanitaire & médico-social).

2. Etat de la menace cyber

« L'heure est grave. Depuis 1 an, tout empire. La cybercriminalité explose, c'est très visible. Pour prendre juste un chiffre : à périmètre constant, on a, en 1 an, un facteur 4 du nombre de victimes en plus. On comptait une cinquantaine de victimes en 2019, en 2020, nous sommes à près de 200. C'est absolument colossal. » Guillaume Poupard, ANSSI

Typologie de la menace

Collectif SI médico-social ARA

Définitions :

« *une action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support* »

A. Coustillère, vice-amiral chargé de la cyberdéfense française

« *tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (secrets militaires, diplomatiques ou industriels, données personnelles bancaires, etc.), de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information (dont les systèmes industriels)* »

ANSSI

Auteurs :

- 20 % cybermafias (dvmt de propres outils)
- 26 % groupes de pirates
- 26 % cybercriminels (achat de service de piratage)
- 17 % de script kiddies
- 8 % de collaborateurs internes

Cibles :

- ordinateurs, serveurs, isolés ou en réseaux, reliés ou non à internet
- équipements périphériques
- appareils communicants (TPH, tablettes…)

4 types de risques cyber :

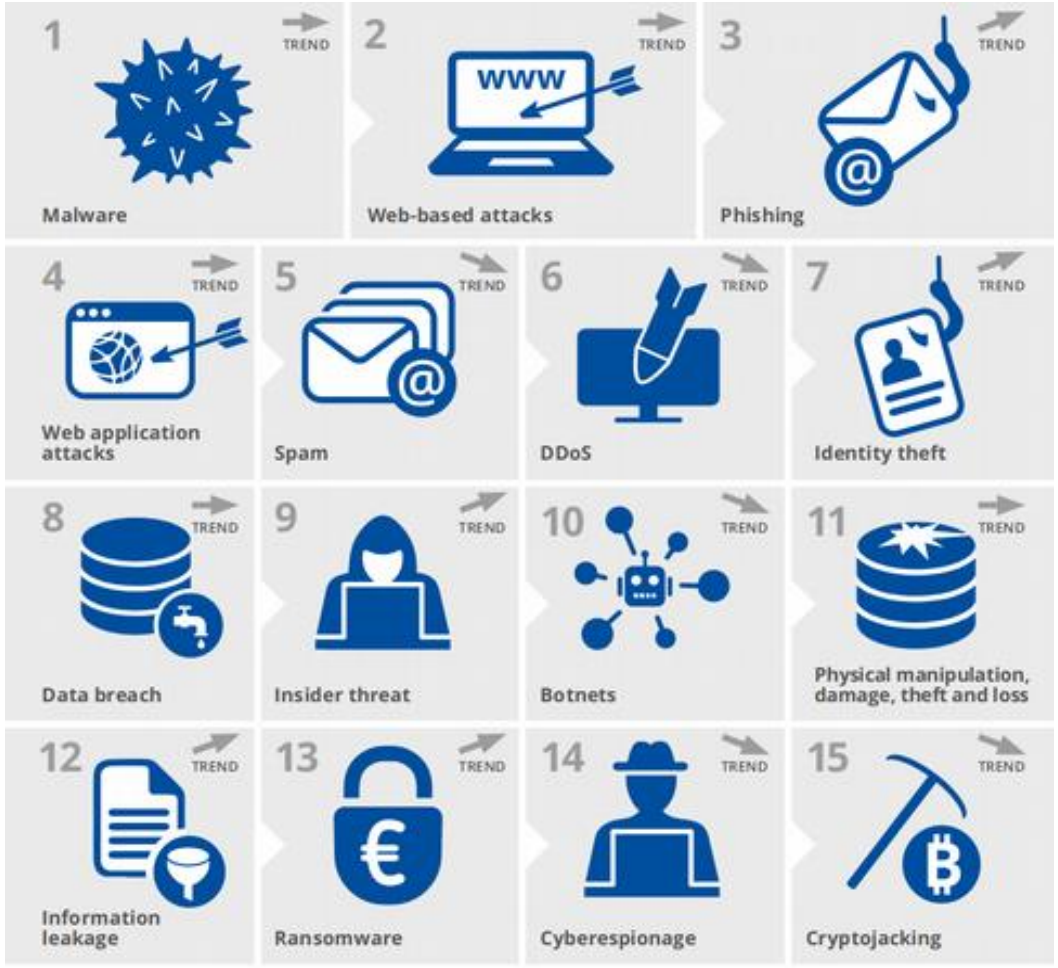
- piratage
- atteinte à l'image
- espionnage
- sabotage

Secteurs ciblés fonction de :

- dépendance à l'automatisation et au numérique
- retard en matière de cyber-résilience
- insuffisance dans les procédures type PCA
- conjoncture : secteur de la santé

Top 15 des cybermenaces *(source ENISA)*

Collectif SI médico-social ARA



Rapport de l'agence de l'UE pour la cybersécurité du 20 octobre 2020 :

***« les cyberattaques deviennent désormais plus sophistiquées, ciblées, massives et non détectées»*.**

10 enseignements à retenir

1. Nouvelle phase de transformation du numérique donc nouveaux défis.
2. Dépendance accrue du cyberespace après la pandémie COVID-19.
3. Utilisation des plateformes de médias sociaux comme cibles des attaques cyber.
4. Véritable organisation du crime avec des attaques finement ciblées et persistantes sur des données de grande valeur (par exemple, propriété intellectuelle et secrets d'états) – parrainage étatique.
5. Attaques distribuées massivement avec une courte durée et un large impact pour organiser le vol d'informations d'identification.
6. Motivation financière derrière la majorité des cyberattaques.
7. Ransomware en forte augmentation avec des impacts financiers élevés.
8. Cyberattaques détectées : partie immergée de l'iceberg.
9. Dimension humaine : principal maillon de vulnérabilité.
10. Automatisation des systèmes de sécurité encore insuffisant.

Conséquences d'une cyberattaque

Collectif SI médico-social ARA

Activité impactée :

- Interruption totale ou partielle d'un élément ou de la totalité d'une chaîne logistique, de production, de gestion … en fonction du secteur d'activité.
Exemple : incapacité dans la gestion des dossiers médicaux des patients.
- interruption du site internet.
Exemple : qui d'une attaque de doctolib sur l'activité des médecins ayant ainsi sous-traité la prise de RDV.
- Ré-allocation des moyens pour gérer la crise et donc baisse de la productivité.
- Stress et surmenage des collaborateurs.
- Management remis en cause pendant et après la crise.

Réputation atteinte :

- Court terme (exemple cours de bourse, risque d'acquisition…).
- Moyen terme (perte de patientèle…).
- Long terme (impact de la crédibilité).

Risque juridique :

- Recours en responsabilité civile voire pénale.

Pérennité de l'entité attaquée en jeu

Sanitaire : secteur impacté

Collectif SI médico-social ARA

« les hôpitaux et autres entités du secteur de la santé représentent l'une des cibles privilégiés des attaquants »

État de la menace rançongiciel – ANSSI – 01/02/2021

Pourquoi ?

- Infrastructure critique, cible naturelle en temps « normal »
- Effet d'aubaine : mise en place TV travail = augmentation de la surface d'attaque dont les conséquences avec la crise COVID19 en accroit la criticité.
- Établissements de santé : faible niveau de sécurité numérique et milieu par définition ouvert (vulnérabilité pour intrusion également physique).

Comment ?

- 70 % des attaques = attaques par rançongiciel.
- Intensification de la menace depuis 2019.
- En 2020, 8 % des attaques par rançongiciel concernait le secteur de la santé. Avec 3 hôpitaux en ZGN.
- En 2021, la RAURA est également touchée (Villefranche sur Saône 15/02/2021) avec paralysie ou forte perturbation du site web de l'hôpital, des standards téléphoniques, de la gestion des patients avec comme conséquence notamment des déprogrammations des opérations chirurgicales.

Collectif SI médico-social ARA

Mode opératoire : 4 étapes

❶Identification du vecteur d'infection :
› courriel piégé ;
› clé USB ou support numérique infecté ;
› site internet piégé (visite d'un site légitime compromis, fausse mise à jour de navigateur par exemple) ;
› vulnérabilité humaine et matériel (VPN ou logiciel vulnérable).

❷ Distribution via :
› intrusion ;
› vol de données ;
› évaluation de la rançon.

❸Déclenchement du rançongiciel (activation du chiffrement des données).

❹Blanchiment quand la rançon est payée.

Conséquences :

› Désorganisation de la planification du service de personnel.
› Difficulté de prise en charge de patients.
› Impossibilité d'utiliser du matériel et de procéder à des commandes.
› Impossibilité de consulter les dossiers de patients…

3. Organisation Gendarmerie & Police

Collectif SI médico-social ARA

Réseau gendarmerie CYBERGEND

National

Centre de lutte contre les Criminalités Numériques (C3N)

Enquêteurs en Technologies Numériques (N'Tech)

Régional et départemental

Sections de recherches – Groupes Cyber (Antenne C3N – N'Tech)

Sections Opérationnelles de Luttes contre les Cybermenaces (SOLC - N'Tech)

Local

Correspondants en Technologies Numériques (C-N'Tech)

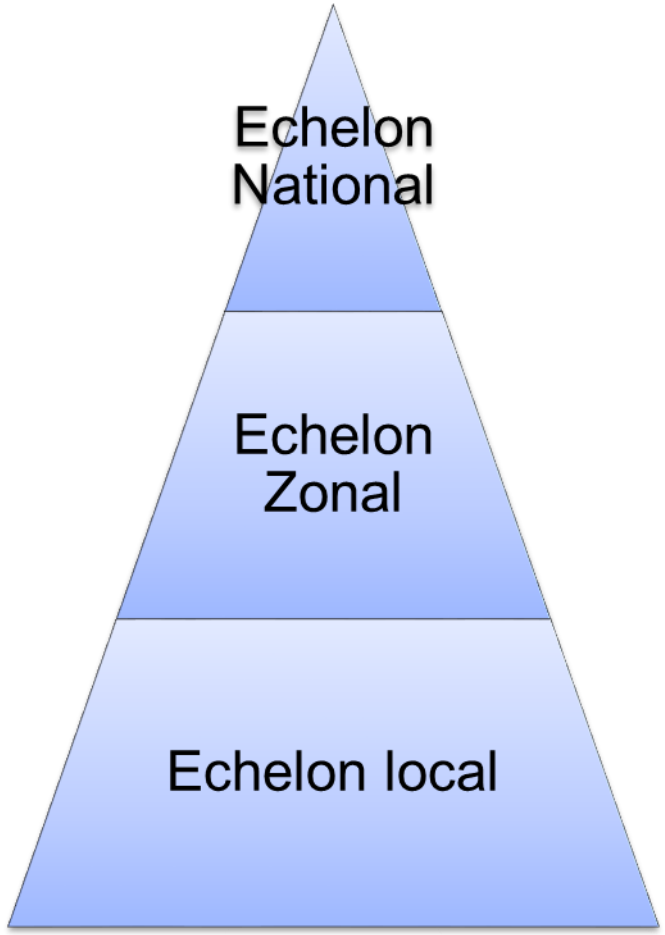
Tout gendarme de terrain

Le maillage cyber de la Police nationale

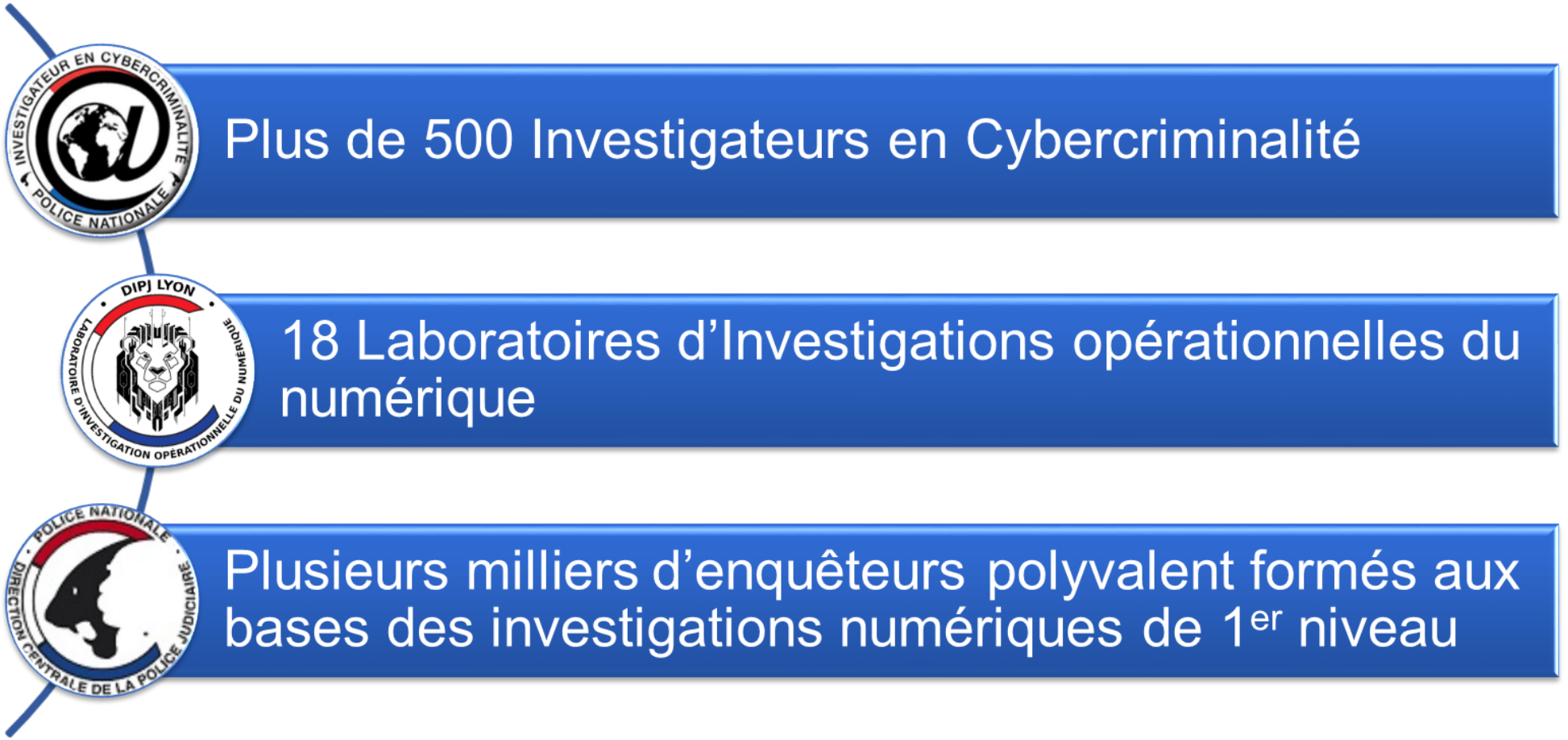
Sous Direction de lutte contre la Cybercriminalité S.D.L.C.

Laboratoires d'analyses opérationnelles du numérique L.I.O.N.

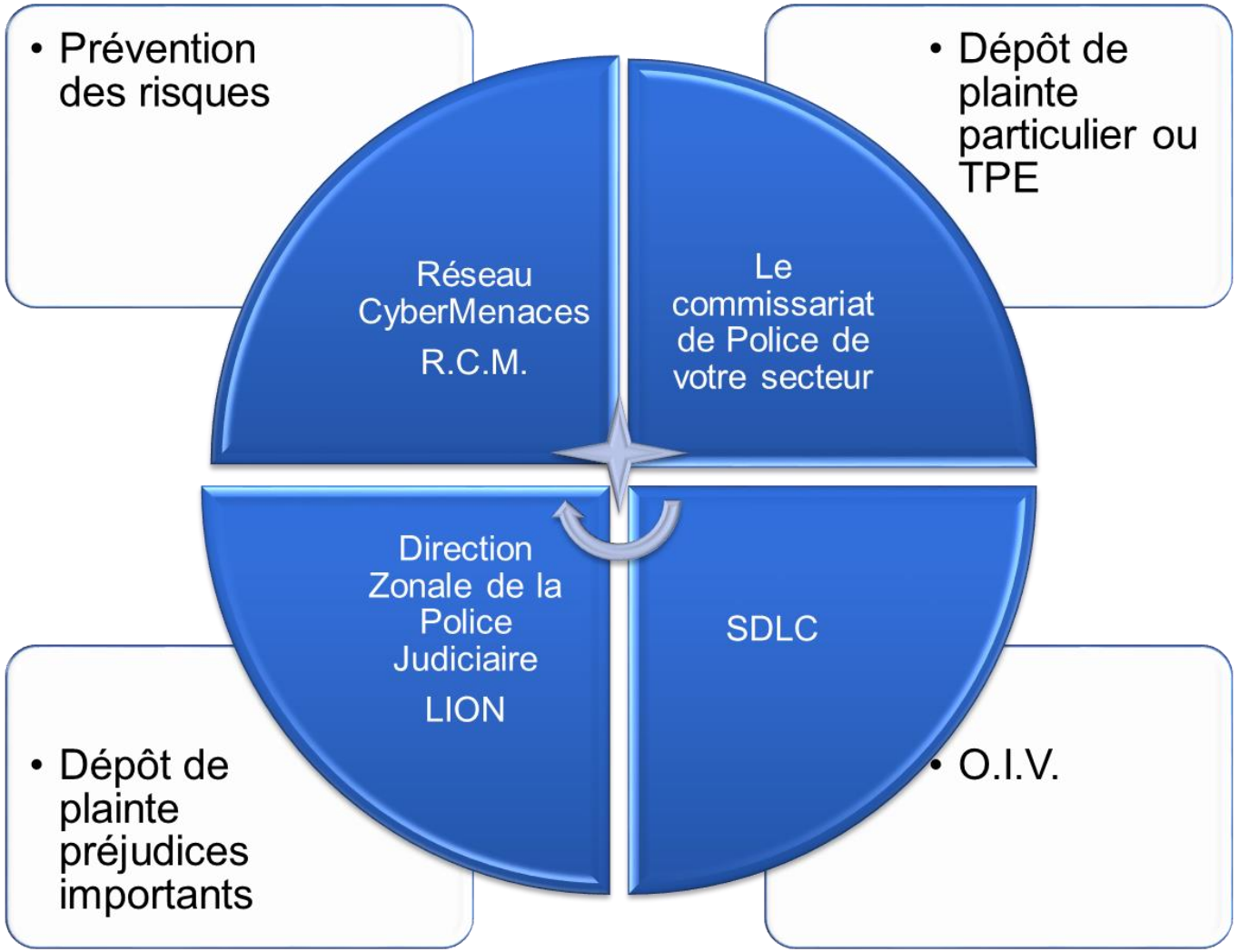
Investigateur en Cybercriminalité I.C.C.et Primo intervenants en Cybercriminalité P.IC.C.



Collectif SI médico-social ARA



Différents niveaux d'interlocuteurs Police

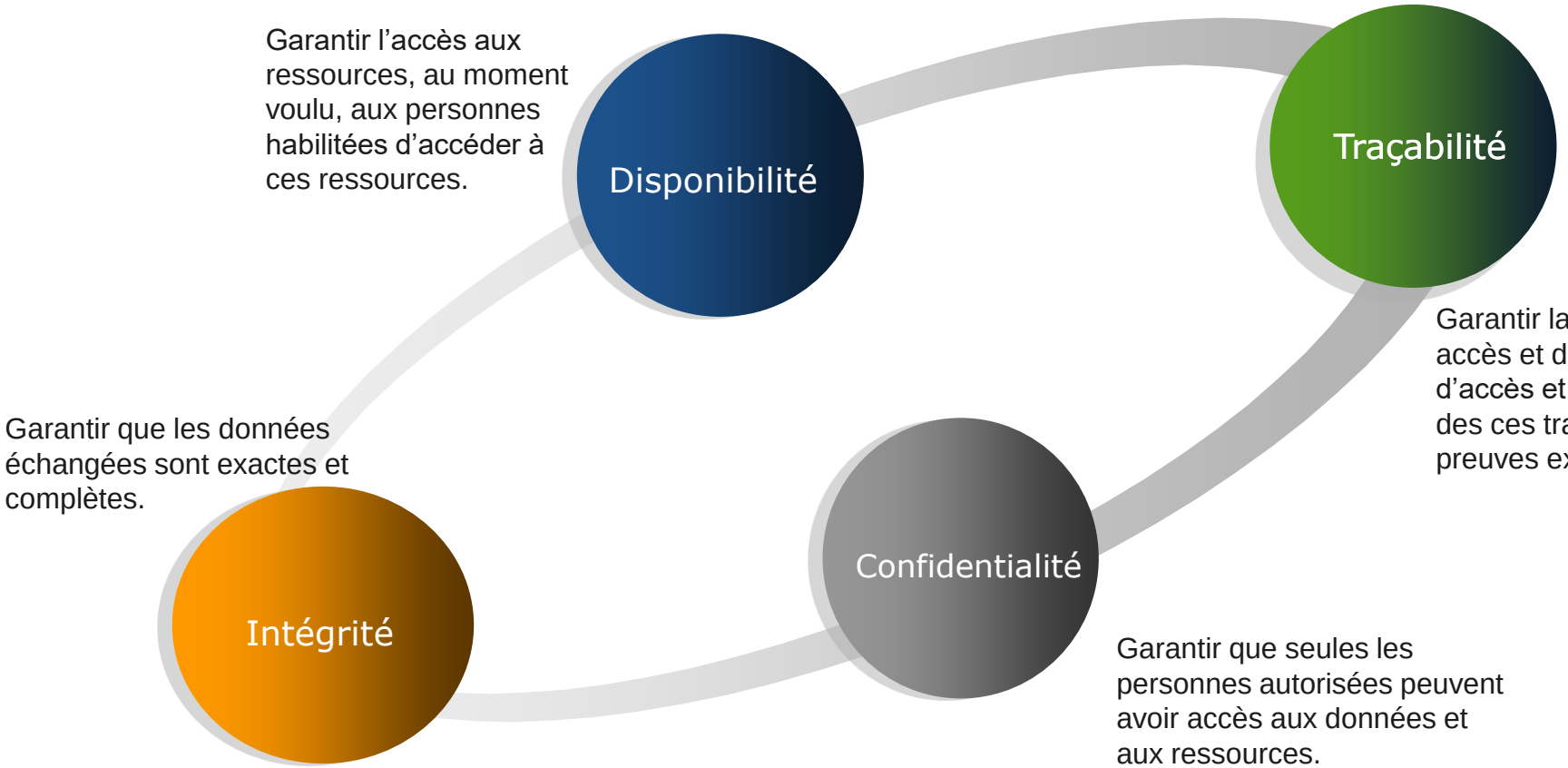


4. Politique de prévention

La SSI, qu'est ce que c'est ?

Collectif SI médico-social ARA

Face aux risques identifiés, ce concept recouvre l'ensemble des mesures prises en vue d'assurer :



--> des informations et du système d'information

Collectif SI médico-social ARA

COMPRENDRE LE RISQUE NUMÉRIQUE ET S'ORGANISER

ÉTAPE 1. Définir un cadre de gouvernance du risque numérique

ÉTAPE 2. Comprendre son activité numérique

ÉTAPE 3. Connaître son seuil d'acceptation des risques

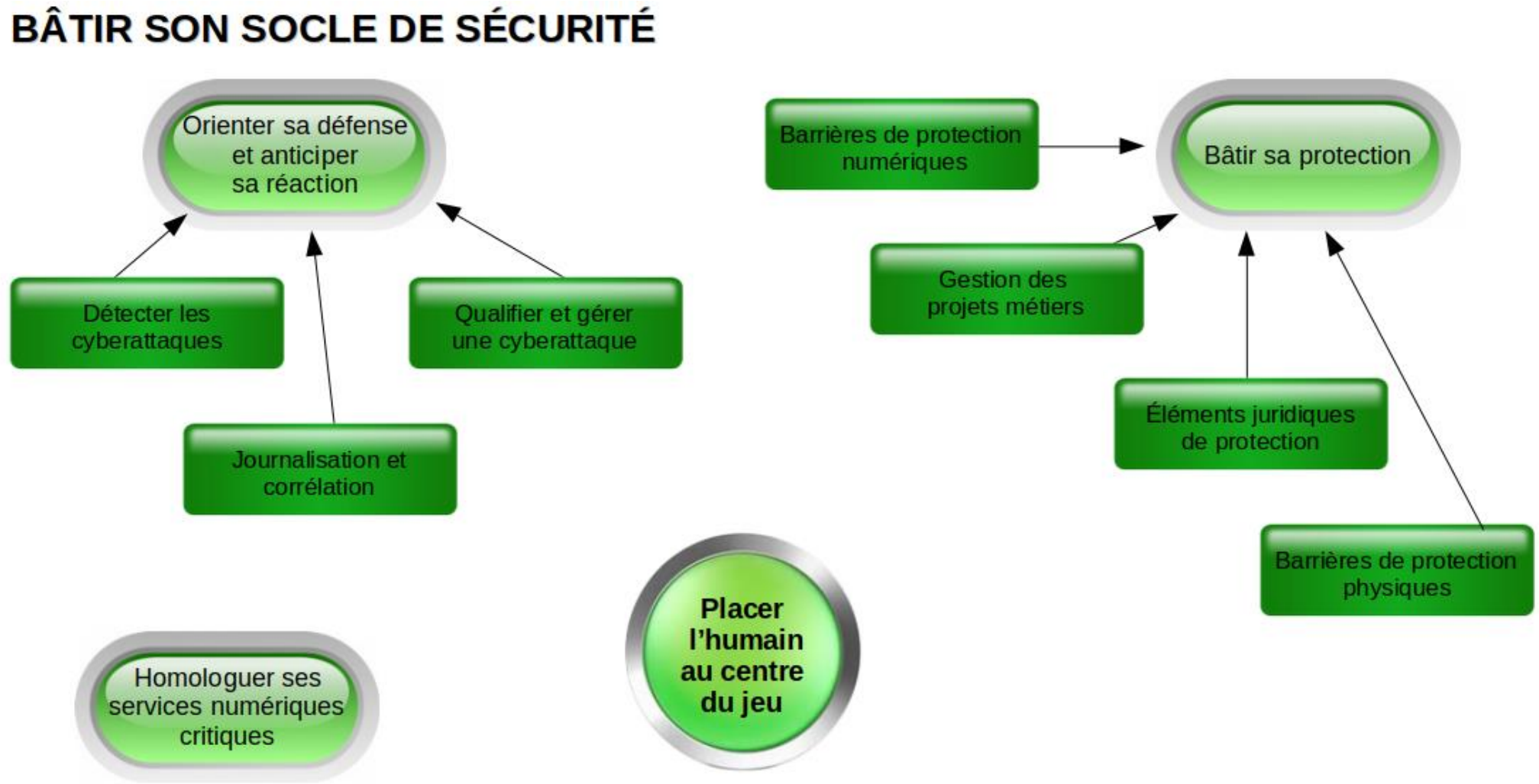
ÉTAPE 4. Construire ses pires scénarios de risque

ÉTAPE 5. Définir sa stratégie de sécurité numérique et de valorisation

ÉTAPE 6. Mettre en place des polices d'assurance adaptées

Prévention 2

Collectif SI médico-social ARA



5. Les réactions en cas d'attaque

La réponse en cas d'attaque

Collectif SI médico-social ARA

Collectif SI médico-social ARA

- En cas de détection d'une cyber attaque, des mesures réflexes doivent être mises en œuvre :

  - **Déconnecter** immédiatement la ou les machines concernées du réseau sans les éteindre.
  - **Alerter** les services informatiques (ou votre prestataire) qui mèneront les actions de confinement, d'investigation et de remédiation.
  - Renouveler immédiatement les mots de passe des comptes concernés, voire ceux des administrateurs si besoin.
  - **Déclarer l'incident sans attendre :**

    1) sur le portail Cyberveille.

    1) en parallèle, via un dépôt de plainte.

    2) à la CNIL s'il y a eu violation et/ou destruction de données à caractère personnel (ensuite, si besoin).
  - **Si un rançongiciel est impliqué, ne procéder à aucune action vers les attaquants** avant d'avoir eu un contact avec les forces de l'ordre ou les services nationaux (CERT-Santé ou ANSSI).

- **Se reporter aux deux fiches réflexes de l'Agence du Numérique en Santé : « Réagir à un acte de cybermalveillance » (directeurs) & « Agir contre un maliciel » (SI & RSSI).**

L'obligation de signaler
1) Cyberveille

- **Le signalement à l'ARS et aux autorités nationales : un des premiers réflexes lors de la détection d'une cyberattaque, en parallèle du dépôt de plainte.** Réflexe installé depuis 2017 au sein des établissements de santé.

- Fin 2020, introduction d'une **obligation de signalement des incidents SI pour les établissements médico-sociaux.** Un décret est attendu pour préciser les modalités de signalement par les établissements, et leurs modalités de traitement.

- Dans l'attente, **tout signalement doit être réalisé sur la plateforme Cyberveille** de l'Agence du Numérique en Santé : https://www.cyberveille-sante.gouv.fr/ (ou directement via le portail de signalement des événements sanitaires indésirables : https://signalement.social-sante.gouv.fr/).

1) Cyberveille

https://www.cyberveille-sante.gouv.fr/

Collectif SI médico-social ARA

Ministère des Solidarités et de la Santé

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé (Cellule ACSS)

ACCUEIL | ACTUALITÉS | ESPACE DOCUMENTAIRE | AIDE AU SIGNALEMENT | LIENS UTILES | CYBER-SURVEILLANCE | CONTACT | SE CONNECTER

Abonnement au flux d'alertes

Connexion

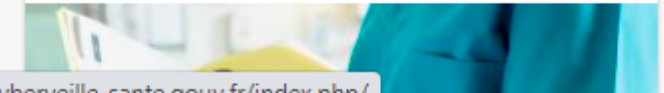
Email or username

Password

Forgot your password?

Actualités

Espace documentaire



CYBERVEILLE SANTÉ

[États-Unis] Le groupe hospitalier Scripps Health victime d'une cyberattaque
Dernière modification le : Mercredi 23 juin 2021 - 16:26

[Nouvelle-Zélande] Plusieurs établissements de santé victimes d'une cyberattaque
Dernière modification le : Mardi 1 juin 2021 - 17:18

Une cyberattaque paralyse le système de santé publique irlandais
Dernière modification le : Vendredi 21 mai 2021 - 19:05

Webinaire sur les actions préventives pour réduire le risque de compromission massive en cas d'attaque par rançongiciel.
Dernière modification le : Mercredi 12 mai 2021 - 17:02

Vulnérabilité sur OpenEMR
Dernière modification le : Vendredi 7 mai 2021 - 15:52

CYBERVEILLE

ABONNEMENT AUX FLUX RSS

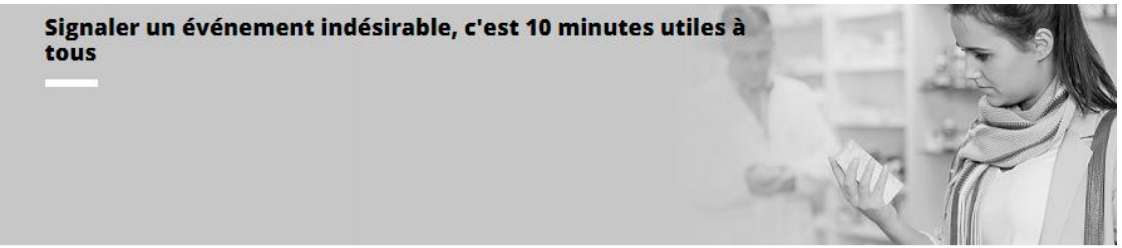
Abonnement au flux RSS Cyberveille

Abonnement au flux RSS Cyberveille Santé

1) Cyberveille

https://signalement.social-sante.gouv.fr/

Collectif SI médico-social ARA



Vous êtes un particulier

Vous êtes la personne concernée, un proche, un aidant, un représentant d'une institution (maire, directeur d'école), une association d'usagers ...

Vous êtes un professionnel de santé

Vous êtes un professionnel de santé ou travaillez dans un établissement sanitaire ou médico-social (gestionnaire de risque, directeur d'Ehpad), ...

Vous êtes un autre professionnel

Vous êtes une entreprise ou un organisme exploitant fabricant, distributeur, importateur, mandataire, ...

- [ ] Gastroentérite Aigue (GEA) - déclaration - 2ème partie
- [ ] Maladies à déclaration obligatoire (MDO)

Cybersécurité

- [ ] Incident de sécurité des systèmes d'information

Vous pouvez cocher un ou plusieurs éléments liés à l'évènement indésirable que vous souhaitez signaler.

PRÉCÉDENT SUIVANT

Ministère chargé de la Santé

Données personnelles et cookies | CGU

Gestion des cookies | Besoin d'aide

Accès évaluateurs

1) Cyberveille

https://www.cyberveille-sante.gouv.fr/

- **Le signalement est transmis :**

  - **à l'ARS.**
  - **aux autorités nationales :** Agence du Numérique Santé (cellule Computer Emergency Response Team Santé ; CERT Santé), Haut Fonctionnaire de Défense et de Sécurité (HFDS) des ministères sociaux. Au besoin signalement également transmis à l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

- **Le CERT Santé apporte, si besoin, un accompagnement dans le traitement de l'incident de sécurité des SI :** proposition de mesures de remédiation, assistance à l'identification de la menace, orientation vers un prestataire de proximité référencé, etc.

  En 2020, près d'1 signalement sur 4 a débouché sur un accompagnement par le CERT Santé.

- La CERT propose également un accompagnement dans la phase d'amélioration des mesures de sécurité : avis sur des plans d'action sécurité, rappels sur les bonnes pratiques, etc.

1) Judiciarisation suite à une attaque par Ransomware

Collectif SI médico-social ARA

Le dépôt de plainte

1) Le dépôt de plainte

Qui ?

- Le chef d'entreprise (ou ayant pourvoir connaissant parfaitement la société).

- Le RSSI (ou technicien ayant les connaissances et compétences relatives à la sécurité du SI et les informations sur l'attaque).

Collectif SI médico-social ARA

Quoi ?

Quelles informations communiquer ?

- Données économiques de la société, données sensibles, impact économique et humain, etc ...
- Données techniques sur le SI et élément de l'attaque.

1) Le dépôt de plainte

Quoi ?

Quelle est l'infraction dont je suis victime ?

Atteinte à un système de traitement automatisé :

- Peine faible ;

- la bande organisée ne concerne que les fichiers mis en œuvre par l'État

Extorsion (tentative) :

- Peine adaptée ;

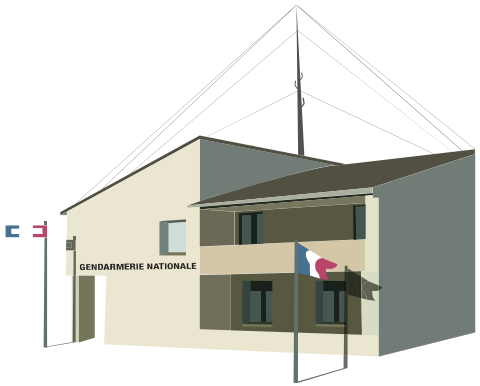
- bande organisée retenue.

Collectif SI médico-social ARA

1) Le dépôt de plainte

À la brigade

Où ?



À la société

Quand ? **IMMÉDIATEMENT**

En parallèle du signalement Cyberveille

1) Le dépôt de plainte

Comment ?

- **Aviser la brigade (commissariat) du ressort et formuler la volonté de déposer une plainte.**

- **La saisine via courrier du service juridique est à proscrire.**

- **La plateforme Thésée (pré-plainte en ligne) n'est pas constitutive d'une plainte.**

1) Après la plainte

Premières investigations :

- Déterminer la racine du logiciel malveillant (ransomware et/ou fichier chiffré).

Saisine du service enquêteur :

- Par parquet de PARIS – 3ème division (JuNaLCO); Section J3 Cybercriminalité ;
- Coopération internationale.

Intelligence économique.

Dispositif PréSAnSCE (Prévention **S**ituationnelle, **An**alyse, **S**écurité et **C**ybersécurité des **E**ntreprises).

2) Notification à la CNIL :

https://notifications.cnil.fr/notifications/index

CNIL.

> Vos démarches > Dépôt de notification

Notification d'une violation de données personnelles

5 étapes pour finaliser votre notification

1	2	3	4	5
TYPE DE NOTIFICATION	ORGANISME	A PROPOS DE LA VIOLATION	ACTIONS ENTREPRISES	RÉCAPITULATIF

2) Notification à la CNIL : https://notifications.cnil.fr/notifications/index

- Tout incident susceptible d'impliquer des **données à caractère personnel et présentant un risque pour les droits et libertés des personnes doit faire l'objet d'une notification à la Commission Nationale Informatique et Libertés (CNIL).**

  Démarche : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
  Notification : https://notifications.cnil.fr/notifications/index

- La notification doit être faite **dans les 72 heures à compter de la découverte de l'incident, avec les éléments suivant** :

  - la nature de la violation et les catégories et le nombre approximatif de personnes concernées par la violation ;
  - les coordonnées du délégué à la protection des données ou toute autre personne responsable ;
  - les conséquences probables et les mesures de remédiations prises ou envisagées.

- **En cas de risque élevé pour les personnes physiques**, la notification aux personnes concernées par la violation **doit se faire dans les meilleurs délais**.

En résumé
Les signalements

1) Prioritairement et de manière concomitante

- **ARS & autorités nationales (Agence Nationale de Sécurité des SI & CERT-Santé)** : signalement via https://www.cyberveille-sante.gouv.fr/ ou via https://signalement.social-sante.gouv.fr/).

- **Gendarmerie nationale ou Police nationale** : dépôt de plainte auprès de la brigade de gendarmerie ou du commissariat de police du secteur.

2) Ensuite, le cas échéant

- **CNIL**, s'il y a risque de violation et/ou destruction de données à caractère personnel https://notifications.cnil.fr/notifications/index

6. RETours d’EXpérience

Retour d’expérience, Cyber attaque

8 juillet 2021

Association Hospitalière
SAINTE-MARIE

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impacts des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

Contexte Cyber attaque

Cyber attaque identifiée le 02/09/2020

- Depuis le 30/08/2020, des utilisateurs signalaient quelques mails de Phishing étranges (situation classique et récurrente, ces signalements étaient consignés)
- Accélération du nombre de mails de Phishing reçu avec des expéditeurs et du contenu de mails AHSM avec notamment des destinataires et expéditeurs faisant partie de la direction
- Les mails contenaient soit des liens vers des sites internet soit un docx (document Word avec macro)
- Le 01/09/2020 fin d’après-midi, un agent du support informatique clique sur un des mails frauduleux transmis par la direction de son site en mode administrateur sur un des CH de l’AHSM
- Le 02/09/2020 matin l’agent du support signal au RSSI son erreur
- Le RSSI déclenche une réunion d’urgence avec le responsable d’exploitation et le responsable du support informatique
- Escalade au DSI

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

Décisions

et actions

- Réflexe de décision : la compromission d'un code administrateur a conduit au déclenchement de la crise.

- Mise en place d'une organisation d'une cellule de gestion de crise informatique dès le 02/09/2020 à 13h00

    - Quantification du niveau de crise : niveau de risque estimé à 4/5 du fait de la compromission d'un code administrateur de domaine Windows.
    - Mise en place d'un plan d'actions avec identification des priorités
    - Recours à une expertise externe : Orange cyberdéfense
    - Contrôle permanent des logs des équipements de sécurité
    - Tenue d'une main courante : tracer à la main tous les éléments importants

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

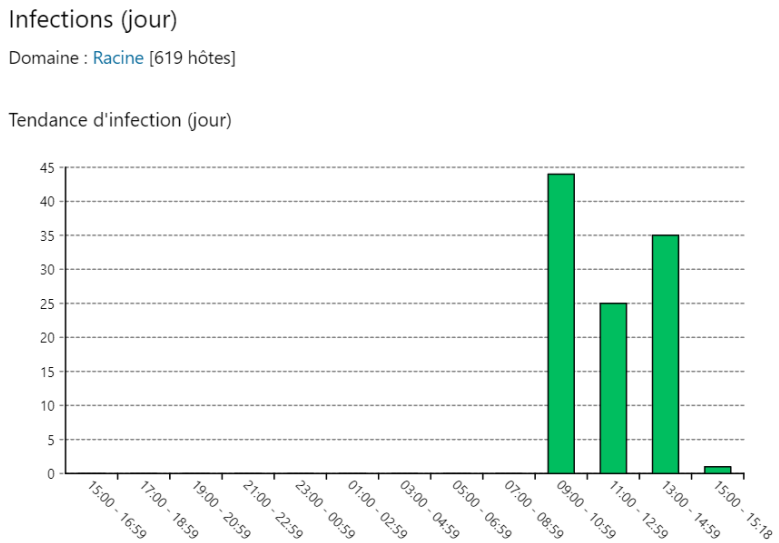
Association Hospitalière
SAINTE-MARIE

• Typologie des virus

Type de virus et impacts

- Dans ce type de situation, il est primordial d'identifier au plus le type de virus et son impact :

  - Or ce virus était mal ou non identifié par nos systèmes anti-virus
  - Nous avions peu d'information sur l'étendue de la propagation
  - Nous avions les traces d'une campagne de Phishing massive vers les boites mails de nos 5 CH.
  - Nous avions l'information d'ouverture d'une pièce jointe Word avec Macro par un administrateur d'un CH
  - Puis les anti-virus se sont affolés signe d'une propagation

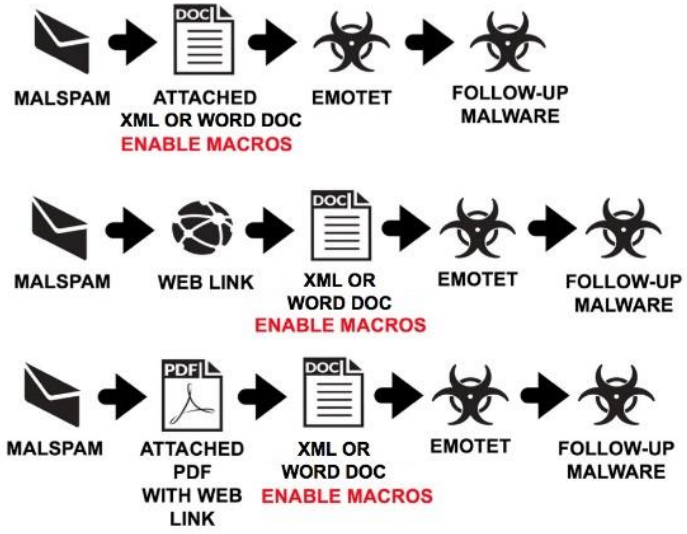


• Typologie des virus

Type de virus et impacts

- Suite à une mise à jour des serveurs AV , le virus Qakbot/Qbot est détecté le 02/09/2020
- Décision d'appel à un expert Cyber compte tenu de la menace. L'expert (OCD) identifie un autre virus le virus EMOTET (installé par la macro Word) , lui-même conduisant à l'installation de Qakbot/Qbot.

Mode de propagation :



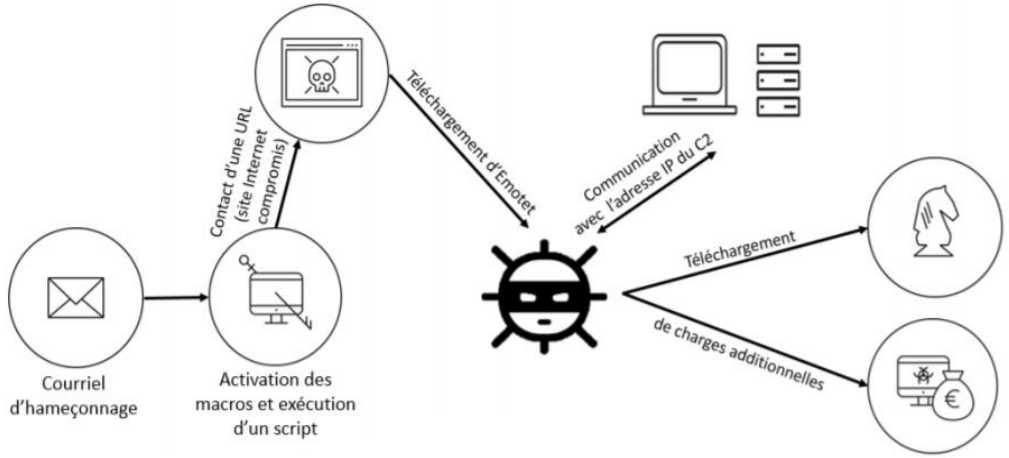


Fig. 2.2 : Chaîne d'infection

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

Expert cyber

- L’expert cyber (OCD) :
  - Recommande une déconnexion des postes infectés d’internet
  - Recommande un formatage de PC infectés
  - Indique que l’étape suivante est la diffusion d’un Ransomware avec blocage du SI
  - Crée un script de désinfection à déployer sur l’ensemble du parc (1000 postes lourds & 300 serveurs), l’antivirus n’étant pas assez efficace.

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

Actions internes et externes

- Principales actions

  - Coupure des accès internet
  - Coupure des flux applicatifs
  - Restriction de la messagerie (blocage des mails entrants, puis des mails avec pièces jointes), redirection des mails avec pièces jointes dans une boite mail de quarantaine pour analyse manuelle avant distribution (+ 3000!)
  - Travaux d'éradication et de propagation du virus (formatage des postes infectés, scripts de désinfection)
  - Déclaration de l'incident auprès de la cellule cybersécurité santé (ACSS, appelé maintenant le CERT Santé: Computer Emergency Response Team)

- Mise en place de solutions de contournement pour les utilisateurs

  - Salles internet
  - Prêt d'ordinateurs portables
  - Gestion manuelle des flux sensibles
  - Whitelist des sites internet autorisés
  - Déblocage manuel des mails en quarantaine

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

• Impact des virus sur le SI de l'AHSM

SI de l'AHSM

- Diffusion des deux virus sur la quasi-totalité d'un parc et des serveurs d'un CH
- Diffusion plus restreintes sur 20 postes d'un autre CH
- Du fait de la segmentation les 3 autres CH n'ont pas été impactés
- Précisions :
  - Les utilisateurs n'ont pas été impactés dans leur utilisation, à part la réception de mails de plus en plus ciblés,
  - Les applications ont continué a fonctionner normalement

L'attaque aurait donc pu passer inaperçue encore un certain temps.

La coupure des mails et des accès internet ont perturbé le bon fonctionnement des ETS mais peu car le DPI n'a pas été impacté et a pu fonctionner normalement.

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

• Actions post-crise & Bilan

Du 30/09/2020

à aujourd'hui

- Cellule de crise clôturée le 30/09/20
- Durée 28 jours
- Un ensemble de travaux sont toujours en cours :
  - amélioration des pratiques d'administration
  - mises à jours
  - renforcement de la veille sécurité et de la surveillance
  - un Retex et un plan d'action ont été effectués

- Le retour progressif du niveau de service à la normale à pris beaucoup de temps, chaque flux internet ayant été vérifié et rouvert au compte goutte.

Ordre du jour

1. Survenue de l'attaque
2. Mobilisation & cellule de crise
3. Typologie des virus
4. Recommandations d'actions immédiates
5. Actions
6. Impact des virus sur le SI de l'AHSM
7. Actions post-crise
8. Recommandations

Association Hospitalière
SAINTE-MARIE

• Recommandations

Après 2020

- Sensibiliser les utilisateurs en amont
- 90 % des attaques passent par la messagerie, il faut donc vraiment sécuriser la réception des mails
- Les antivirus classiques ne suffisent plus (les virus avaient traversé 3 antivirus différents)
- Face à un incident de sécurité SI, il faut réagir vite et être attentif aux premiers signes
- Effectuer, vérifier et **isoler** ses sauvegardes (seuls rempart contre les Ransomwares)
- Les informaticiens peuvent être aussi malgré eux vecteur d'une attaque, les comptes d'administration doivent être utilisés avec précautions.
- Ne pas hésiter à faire appel rapidement à des experts sécurité en cas de crise
- Se préparer à la gestion de crise cyber (exercices, fiches réflexes, définir une cellule de crise multi métiers pas uniquement DSI)
- Ne pas se dire que cela n'arrive qu'aux autres mais se dire que cela va forcément se produire…..

- Mise à jour: Une bonne nouvelle le réseau EMOTET démantelé en janvier 2021 par Europol, mais le Ransomware Conti à pris la suite…

Merci
pour votre attention

Questions

Association Hospitalière
SAINTE-MARIE

Groupement de Coopération Sanitaire
du Roannais

Webinaire cybersécurité

08/07/2021

Retour d'expérience – GCS du Roannais

Rappel de l'événement

Dans la nuit de samedi 18 janvier au dimanche 19 janvier 2020, **un logiciel malveillant *(de type CryptoLocker)* a exploité une faille de sécurité du logiciel de monitoring du prestataire informatique (contrat groupé GCS) pour se propager dans les systèmes d'exploitation des établissements**

Les conséquences

- Ensemble des documents et fichiers des serveurs internes de stockage cryptolockés

- Inaccessibilité des logiciels métiers en réseau entre J5 et J15

Les conséquences

- Si sauvegarde externalisée : récupération des données entre J10 et J15

- En l'absence de sauvegarde externalisée : aucune restauration possible, perte totale des données des fichiers bureautiques

- Délai de remise en route des logiciels métiers entre J5 et J15

Nos actions immédiates

- Déclaration de l'évènement : Portail de signalement ARS (20/01/2020) et Cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS) (23/01/2020)

- Déclaration CNIL concernant la violation de données personnelles (28/01/2020)

- Dépôt de plainte contre X auprès des services de police /gendarmerie

- Retour d'information -> Administrateur du GCS du Roannais pour coordination des actions vis à vis du prestataire informatique (sans suites de sa part)

Actions à court terme

- Report des activités administratives nécessitant des accès logiciels, information des tiers concernés
- Mise en place immédiate de la procédure dégradée pour les soins (ordonnances, plans de soins papier, fiches de traçabilité)
- Remise en route immédiate d'une sauvegarde locale sur disque dur externe

Nos actions à plus long terme

- Souscription du contrat de sauvegarde externe (hébergement DATA CENTER)
- Obtention d'un document faisant l'état des lieux de protection des systèmes d'informations, de la part du prestataire – 30 mars 2021
- Réflexion engagée au niveau du GCS / échéance du contrat de prestation 07/2023 + GT SI au sein du GCS
- Inscription ANSSI dans le cadre du Plan France Relance cybersécurité ?

En conclusion

En conclusion
Un risque comme les autres

- En dépit de son caractère imprévisible et technique, le risque cyber peut être prévenu, voir évité (intérêt de la prévention) ou ses conséquences peuvent être limitées : c'est l'objectif d'une politique de maîtrise de risques.

- Le plan de renforcement 2021 de la cybersécurité encourage la prise en compte du risque cyber, dans la lignée de **la Politique Générale de Sécurité des Systèmes d'Information – Santé (PGSSI-S)**, promue depuis 2012, et qui constitue une **politique d'accompagnement à la mise en place d'un système de gestion des risques numériques**, comme on peut le trouver dans un Plan de Continuité d'Activité (PCA) pour les autres types de risques.

- La PGSSI-S vise à guider les acteurs des secteurs santé & médico-social dans l'appréhension et la compréhension de la réglementation qui leur incombe en matière de sécurité numérique. Elle fixe les grandes orientations en matière de sécurité des SI. Elle leur permet également d'être informés des bonnes pratiques (référentiels, guides, etc.).

Plus de détails en fin de présentation, à consulter.

En conclusion
Un risque comme les autres

- **Une gestion des risques liés au numérique ne repose pas uniquement sur des solutions techniques : elle est également dépendante du système global de gestion des risques.**

- En l'absence de PCA ou de Plan de Continuité Informatique (PCI), **mettre en place des procédures de gestion de crise** :

  - formaliser la mise en place d'une cellule de crise (composition/missions),
  - fiche réflexe sur la transmission de l'alerte (interne/externe),
  - mise en place de procédures dégradées en cas de SI non-fonctionnels (récupération de sauvegardes, passage au papier)…

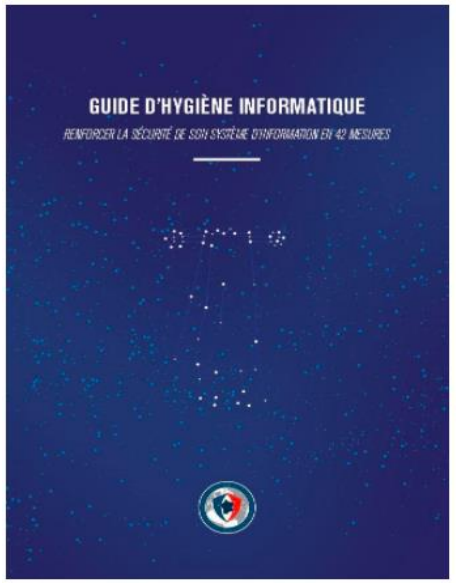
- Dans la mesure du possible, il convient de profiter de la réflexion sur le risque cyber pour enclencher une démarche plus générale de gestion des risques, au sein de laquelle s'intégrera le risque cyber.

Pour finir : les outils à disposition

Les ressources de l'ANSSI

Collectif SI médico-social ARA

Retrouvez ces guides et plus encore sur le site de l'ANSSI : https://www.ssi.gouv.fr



https://sisse.entreprises.gouv.fr/fr/ressources/documentation

Des référentiels, des guides, des plaquettes : ces documents à télécharger sont édités pour vous sensibiliser aux notions de cyber-sécurité, aux concepts, aux méthodes pour déterminer, défendre et promouvoir activement nos intérêts stratégiques.

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Plusieurs outils & ressources proposés par Cyberveille, en complément de l'accompagnement dans le traitement de l'incident :

- **Espace documentaire permettant le partage de guides, fiches pratiques et autres documents utiles.** *Exemples : fiche prévention « maliciel », fiche réflexe « déni de service », fiche réflexe « réagir à un acte de cybermalveillance », fiche prévention « sécuriser son exposition Internet », etc.*

- Des alertes « Cyberveille » & « Cyberveille Santé » permettant d'informer et d'alerter sur des vulnérabilités ou des dysfonctionnements de dispositifs médicaux ou de technologies de santé, sur des actes de cyber-malveillance, etc. Des recommandations de conduite à tenir sont aussi communiquées. Possibilité d'abonnement au flux d'alerte et aux flux RSS.

MOOC SecNumAcadémie

https://www.secnumacademie.gouv.fr/

Collectif SI médico-social ARA

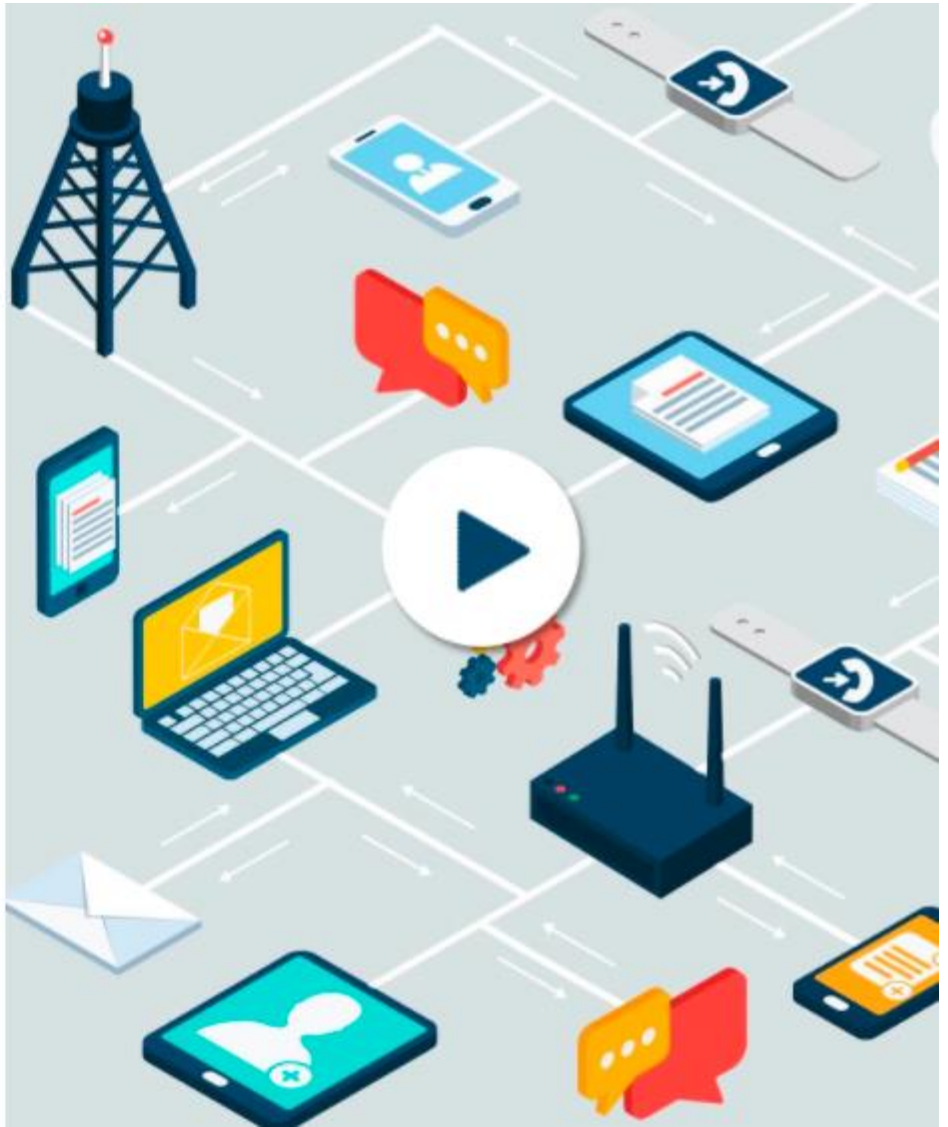
SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

Bienvenue sur le MOOC de l'ANSSI.

Vous y trouverez l'ensemble des informations pour vous **initier à la cybersécurité**, approfondir vos connaissances, et ainsi **agir efficacement sur la protection de vos outils numériques**. Ce dispositif est accessible gratuitement. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

Accéder au MOOC de l'ANSSI

MENTIONS LÉGALES | DONNÉES PERSONNELLES | F.A.Q.



Collectif SI médico-social ARA

- **SecNumacadémie est un programme en ligne de sensibilisation à la sécurité du numérique.** Vous pourrez vous initier à la cybersécurité, approfondir vos connaissances, et ainsi agir sur la protection de vos outils numériques. Ce dispositif est **accessible à tous gratuitement**.

- 4 modules de 5 unités chacun (environ 2 jours en tout), portant sur :

- Panorama de la SSI
- Sécurité de l'authentification
- Sécurité sur Internet
- Sécurité du poste du travail et nomadisme

- Le suivi de ce dispositif vous fera bénéficier d'une attestation de réussite, délivrée par l'ANSSI.

La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)

https://esante.gouv.fr/securite/politique-generale-de-securite-des-systemes-d-information-de-sante

- **La PGSSI-S, élaborée depuis 2012, vise à guider les acteurs des secteurs santé & médico-social dans l'appréhension et la compréhension de la réglementation qui leur incombe en matière de sécurité numérique.** Elle fixe les grandes orientations en matière de sécurité des SI. Elle leur permet également d'être informés des bonnes pratiques.

- Concrètement, la PGSSI-S est un **corpus documentaire**, conforme au cadre juridique de la santé numérique, régulièrement mise à jour et enrichie, **qui vise à établir un cadre dans la définition des niveaux de sécurité attendus et dans la mise en œuvre de la politique de sécurité SI.**

- Ce corpus documentaire est composé de documents se présentant par paliers : palier minimal & paliers progressifs, permettant une amélioration progressive de la sécurité. Vous y trouverez :

- **Des référentiels** (fixant le niveau d'exigences et les paliers à atteindre ;
- **Des guides pratiques et des documents d'accompagnement**.

Parmi les guides pratiques, se reporter notamment au **« Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire & médico-social – Structure sans approche SSI formalisée »** :

- Guide destiné aux structures ne disposant pas encore d'approche formalisée pour la SSI, ou aux structures disposant d'une PSSI incomplète ou obsolète.

- Démarche proposant une élaboration et une mise en œuvre progressive, dans une optique d'amélioration continue de la sécurité.

Il s'adresse en priorité aux responsables de structures.

Les références

Textes officiels (ordre chronologique)

- Arrêté du 13 décembre 2016 portant désignation des autorités qualifiées pour la sécurité des SI (…) : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033624998/
- Instruction n°SG/HFDS/DGCS/2017/219 du 4 juillet 2017 relative aux mesures de sécurisation dans les établissements et services sociaux & médico-sociaux : https://www.legifrance.gouv.fr/circulaire/id/42445
- Ordonnance n°2020-1407 du 18 novembre 2020 relative aux missions des ARS : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042532916
- Article L1111-8-2 du Code de la Santé Publique : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036515017/2018-01-19

Références : focus sur les directeurs d'ESMS et leur rôle

- **Arrêté du 13 décembre 2016 portant désignation des AQSSI (…)**

- Il désigne comme Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI) les « directeurs des (…) établissements publics et des organismes placés sous la tutelle des ministres » (dont Santé & Affaires sociales). Ce sont les directeurs d'établissements médico-sociaux.

- Les AQSSI sont responsables de la sécurité des SI pour leur structure. Elles s'assurent de l'application des instructions ministérielles données en la matière.

- **L'instruction du 4 juillet 2017 relative aux mesures de sécurisation dans les ESMS**

- Elle rappelle aussi le rôle des directeurs d'ESMS dans la sécurisation des SI, et notamment la mise en œuvre des mesures de la PSSI MCAS et de la PGSSI-S.

Collectif SI médico-social ARA

Quelques documents d'accompagnement

- Guide pour réaliser un Plan de Continuité d'Activité, 2013, SGDSN : http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

- Guide pratique - Plan de Continuité Informatique – Principes de base, 2016, PGSSI-S : https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi-s_guide_pci_v1.0.pdf

- Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social – Structure sans approche SSI formalisée, 2015, PGSSI-S : https://esante.gouv.fr/securite/pgssi-s/espace-de-publication (dont focus cartographie des risques SI et cartographie générique)

- Mémento « Cybersécurité » à l'usage du directeur d'établissement de santé, 2017, DGOS : https://solidarites-sante.gouv.fr/IMG/pdf/dgos_memento_ssi_131117.pdf

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