Cybersécurité et ESMS : comment les Centres régionaux de ressources cybersécurité peuvent-ils vous accompagner ?

- Auriane Lemesle, Responsable du pôle cybersécurité, GRADeS PDL
- Margaux Buguet, Responsable de missions, ANS

1. Se préparer à la menace cybersécurité dans le médico-social

2. Témoignage du CRRC des Pays de la Loire

LE VILLAGE DE LA E-SANTÉ

1. Se préparer à la menace cybersécurité dans le médico-social

Le Programme CaRE (Cybersécurité accélération et Résilience des Établissements)

Cybersécurité de la santé | e-santé

Ce programme ambitieux, **dans lequel le médico-social est pleinement intégré**, se décline, sur la période 2023-2027, autour de **4 axes** :

1. **Gouvernance et résilience**
2. **Ressources et mutualisation**
3. **Sensibilisation**
4. **Sécurité opérationnelle**

Délégation de **26 millions €** aux Centres Régionaux de Ressources Cybersécurité (CRRC) dont **18 millions €** pour les objectifs généraux et **8 millions €** pour le **secteur médico-social.**

Trois messages clés

La cybermenace, ça concerne le médico-social !

- *Les ESMS gèrent les données personnelles, voire médicales, **des personnes qu'ils accompagnent**, mais également les données personnelles **de leurs salariés**.*

L'implication de la direction dans le projet, a minima en tant que sponsor, est cruciale.

*« **Une attaque cyber, c'est tout sauf un sujet numérique car, au moment de l'attaque, on n'a plus d'outils numériques** »*

Bastien Le Hyaric, DSI, ADAPEILA

- ***La cybersécurité est un sujet stratégique qui intègre une dimension organisationnelle et métier et qui concerne l'ensemble des professionnels de la structure.** Les professionnels en charge du système d'information ne sont pas les seuls concernés !*
- ***Il est essentiel que les directions s'en saisissent** et définissent des objectifs stratégiques afin d'impulser la démarche et d'aider à la conduite du changement.*

Veiller à anticiper !

- *« En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard » : **mieux vaut avoir réalisé 60% du chemin que ne rien avoir initié.***
- *Le retour à la normale après la survenue d'une cyberattaque ne se fait pas en quelques heures, ni même en quelques jours ! **Les impacts d'une cyberattaque peuvent durer plusieurs mois** (SI à reconstruire,…).*

Par quelles actions puis-je démarrer ?

*« Nous invitons les ESMS à se faire accompagner **par leur CRRC** (centre régional de ressources cyber) car une cyberattaque, ça peut arriver à tout le monde. C'est important de pouvoir **se projeter** et **de connaitre les points où nous sommes en fragilité**. Ça permet également de rendre la cybersécurité **tangible** »*

Directeurs, L'Olivier Bleu

Contacter votre CRRC

- Réalisez un **exercice de crise** et/ ou un **diagnostic de cybersécurité**
- Mettez en place des premières actions **concrètes, structurées et adaptées** à votre contexte
- Disposez d'un suivi régulier afin de vous aider à mettre en place **votre plan d'action**

2. Témoignage du CRRC des Pays de la Loire

Par où et comment démarrer ?

Se préparer

S’évaluer

Agir

S’exercer

Sensibiliser

SE PREPARER

Centre de ressources SSI mutualisées destiné aux ESMS

• Mis en œuvre dès 2022, sur **l'initiative de l'ARS Pays de la Loire**, pour *soutenir les structures ne disposant pas (ou peu) de compétences informatiques internes* et leur permettre *d'augmenter le niveau de sécurité de leur système d'information*.

• Coconstruit avec le **Collectif SI MS** de la région, pour *définir les axes de travail et thématiques prioritaires à prendre en compte.*

• Basés sur les **guides et référentiels nationaux**, pour *aider les structures à les mettre en œuvre et à s'auto-évaluer vis-à-vis de ces derniers.*

Guide cyber dédié au social et médico-social

Référentiels applicables

• Sous l'impulsion du programme CaRE, le périmètre des accompagnements s'étend à l'ensemble des **structures sociales et médico-sociales** de la région adhérentes au Groupement e-santé.

74

structures ont intégré la démarche et bénéficié d'un 1er accompagnement.

86

accompagnements réalisés ou planifiés.

S'EVALUER

Focus sur le diagnostic de maturité de la sécurité du SI

Opportunité de bénéficier d'un **panorama à 360°** sur les **menaces** et d'**un état des lieux** de votre positionnement par rapport aux référentiels nationaux.

Accessible au travers du **centre de ressources SSI mutualisées** à destination des ESMS adhérents du GCS e-santé.

Entretien de 3h (max), en distanciel, avec un intervenant indépendant.

Les diagnostics sont **pris en charge** par l'ARS Pays de la Loire pour les adhérents du Groupement e-santé dans le cadre du programme CaRE.

Ce que ça m'apporte :

- Savoir où je me situe
- Cibler mes priorités
- Faire un état des lieux complet
- Partager les constats
- Mieux comprendre les sujets liés au SI
- Obtenir des livrables personnalisés

S'EVALUER

Les étapes du diagnostic de maturité de la sécurité du SI

Fiche contexte

Entretien téléphonique / visio
15 à 20 min

Entretien du diagnostic

En visio, 3 heures max

Restitution

En visio, 1 heure

1 mois

Objectif :

Recueillir un premier niveau d'informations sur le bénéficiaire et l'organisation de son SI.

Objectif :

Recueillir un maximum d'informations sur le niveau de sécurité du SI du bénéficiaire.

Modalités *:*

Représentant de la structure + Référent SI (interne ou externe).

Aucune action sur le SI par l'intervenant externe.

Livrables remis :

- *Rapport complet (PDF)*
- *Synthèse managériale présentée en séance (PDF)*
- *Outil de suivi du plan d'action (Excel)*

S'EVALUER

Focus sur le diagnostic de maturité de la sécurité du SI

54 diagnostics réalisés.

Pour **90,9%** des répondants, l'accompagnement a totalement répondu à leurs attentes.

« Diagnostic très instructif et utile pour le futur de l'établissement ! Un technicien très pédagogue et à l'écoute. »

Direction - EPSMS

« La compréhension et l'échange autour du plan d'action permettent une amorce rapide et accessible des premières actions d'amélioration. »

Direction - EPMS

« Réelle écoute des questions, reformulation des termes techniques très appréciable. »

Direction - EPMS

« Accompagnement de très bonne qualité. Merci de cette aide précieuse, à recommander à toutes les structures n'ayant pas de service informatique. »

Ingénieur Qualité / Gestion des risques / RSI - EHPAD

« Ce diagnostic a mis en évidence certains dysfonctionnements sur les remontées d'alertes au niveau de notre infogéreur qui ont été corrigé immédiatement. Et accéléré d'autres projets tel que le changement de notre Firewall. »

Chef projet informatique - EHPAD

AGIR

Catalogue des accompagnements disponibles

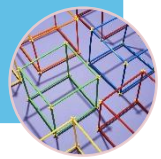
Evaluation du niveau général de maturité de sécurité du SI basée sur un questionnaire, donnant lieu à un plan d'action concret et priorisé.

Diagnostic de maturité de la sécurité du SI

Initiation ou mise à jour de l'inventaire des composants du SI (matériels, logiciels, applications, …)

Note : Modèle fourni

Cartographie du système d'information



Revue des composants essentiels de sécurité du SI : pares-feux, antivirus, sauvegardes, …

Diagnostic des équipements de sécurité

Rappel des bonnes pratiques de revue des pares-feux et révision des règles en place sur votre matériel.

Accompagnement revue des règles de pare-feu

Vérification de la posture de sécurité de votre AD avec plan d'action correctif pour la revue de la configuration.

Diagnostic de l'Active Directory

Vérification du maintien en condition de sécurité et du paramétrage permettant de limiter la réception de messages indésirables et les usurpations d'identité

Diagnostic de messagerie (hors Office 365)

Revue des droits, gestion des utilisateurs, configuration et traçabilité

Diagnostic plateforme collaborative Office 365

Cartographie des données, des technologies utilisées, planification des sauvegardes et restauration

Aide à l'élaboration du plan de sauvegarde

Cadrage technique et plan d'action

Note : test non réalisé en séance, à réaliser a posteriori par la structure.

Préparation réalisation d'un test de restauration

Vérification du niveau de sécurité mis en place sur les Wifi professionnel et usager / résident avec plan d'action priorisé pour la remédiation.

Sécurisation de la configuration Wifi

S'EXERCER

Accompagnement à la réalisation d'un 1er exercice de crise d'origine cyber

Objectifs

- Renforcer la **capacité des établissements à faire face à un incident majeur d'origine cyber, impactant l'activité de la structure.**
- **Augmenter la résilience de l'offre de soins et d'accompagnement**.
- Aider à **identifier les activités critiques** qui seront à traiter en priorité lors de la formalisation **du Plan de Continuité et de Reprise d'Activité** (PCRA).

Accompagnement régional

Une démarche éprouvée sur le secteur sanitaire.

Un KIT documentaire adapté au secteur ESMS (scénario, fiches réflexes, …) avec plusieurs niveaux de maturité.

Une simulation de crise d'environ 1h15 (durée totale de l'exercice 3h)

L'équipe du GCS e-santé, via un prestataire, présent sur site

Ce que ça m'apporte :

Prise de conscience des métiers sur les impacts d'un incident majeur touchant le SI

Sensibilisation concrète à la gestion de crise d'origine cyber

Mise en évidence des axes d'amélioration dans un plan d'action priorisé

S'EXERCER

Retours d'expérience réalisation d'un exercice de crise d'origine cyber

118 exercices sanitaires représentant 99% de l'offre de soins
31 exercices ESMS au bénéfice de 313 structures / sites

L'ARPEP et l'ADAPEI ARIA Vendée nous ont partagé leur témoignage de leur exercice de crise

« Un exercice vivant et réaliste » « quasiment réel ! »
« Il nous a permis d'ouvrir les yeux sur les crises d'origine cyber »
« Apprentissage accéléré »
« Si nous avions réalisé l'exercice nous-mêmes, nous n'aurions pas été aussi loin ! »

Accès aux vidéos

Merci pour leur partage

Les PEP Pays de la Loire La solidarité en action

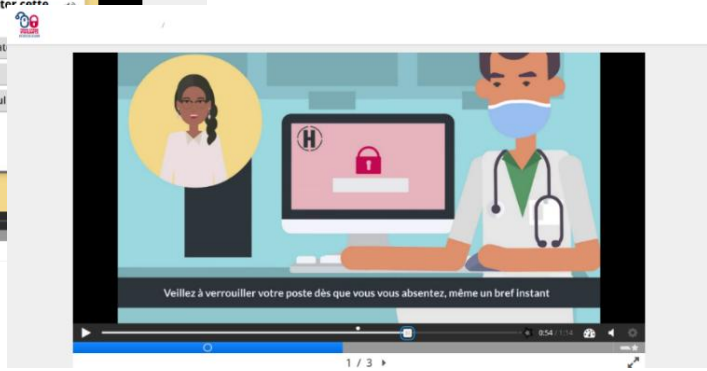
Adapei-Aria VENDÉE AGIR ENSEMBLE FACE AU HANDICAP

TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

SENSIBILISER

Les utilisateurs via e-learning et faux-phishing

- **Répond aux actions liées à la sensibilisation** des utilisateurs aux bonnes pratiques d'hygiène numérique.
- Plateforme permettant la diffusion de **campagnes de e-learning et de faux-phishing à un ensemble de destinataires**.
- Contenus de e-learning **contextualisés aux ESMS.**
- 2 modes d'accès :
  - *Autonome via l'acquisition de licence.*
  - *En mode opéré par le Groupement e-santé PdL.*



SENSIBILISER

Exemples de mails de faux-phishing

Phishing simple
(1 lien à cliquer)

Paiement sécurisé

Cher(e) Client(e),

Votre service client **GlobalExpress** vous informe que vous recevez ce message en dernier avis concernant votre dossier **n°4868.**

En effet, plusieurs tentatives infructueuses de vous joindre sur votre téléphone personnel nous autorise à vous l'adresser.

Nous avons enregistré un double débit sur votre compte client, servant pour la même mensualité comptant pour la somme de 105,90€ (soit 52.95€ x 2).

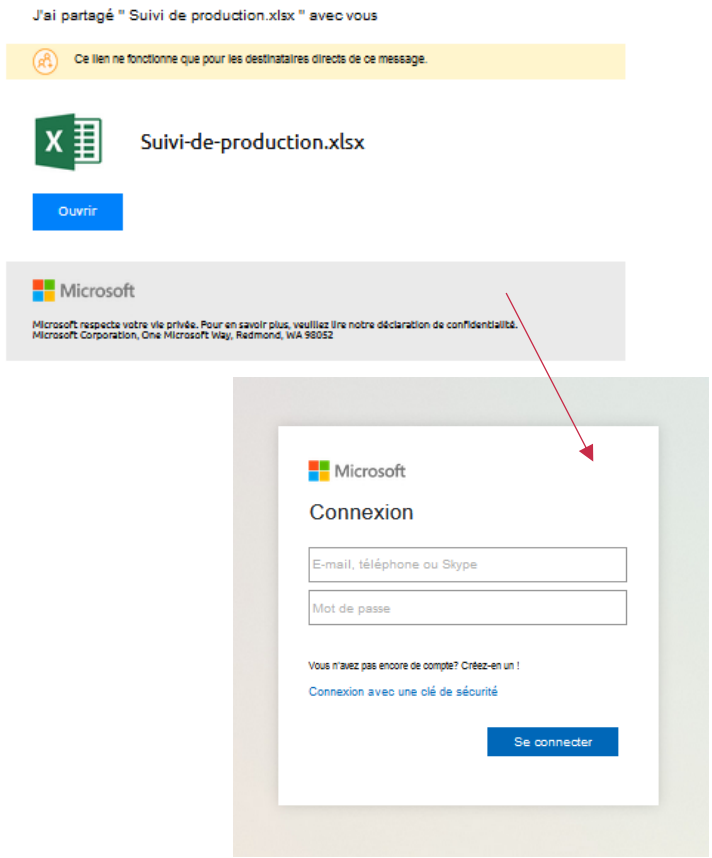
Pour résoudre le problème maintenant et obtenir des informations supplémentaires, UnionExpress reste à votre disposition en cliquant ci-dessous :

Cliquez ici !

Nous vous remercions de votre confiance,

Cordialement,
Votre **service client GlobalExpress**

Phishing avancé
(1 lien à cliquer + 1 page authentification)



Rappel systématique des bonnes pratiques (phishing simple et avancé)

SENSIBILISER

Programme de sensibilisation 2026 - Opéré par l'équipe du GRADeS PdL

Campagnes mensuelles de e-learning :*

Janvier
Faits insolite santé

Février
Réseaux sociaux

Mars
Ransomware

Avril
Identitovigilance

Mai
MSSanté

Juin
Mise à jour

Juillet – Août
Phishing (pièce jointe)

Septembre
Utilisation du mail professionnel sur internet

Octobre
Cybermoi/s

Novembre
Mot de passe

Décembre
Accès aux données sur applications mobiles

+ 4 campagnes de simulation de hameçonnage
(1 par trimestre)

+ remise de rapports trimestriels formalisant le suivi des campagnes

** Durée moyenne des vidéos de e-learning : entre 2min30 et 5 minutes.*

SENSIBILISER

Via des outils ou accessoires de sensibilisation

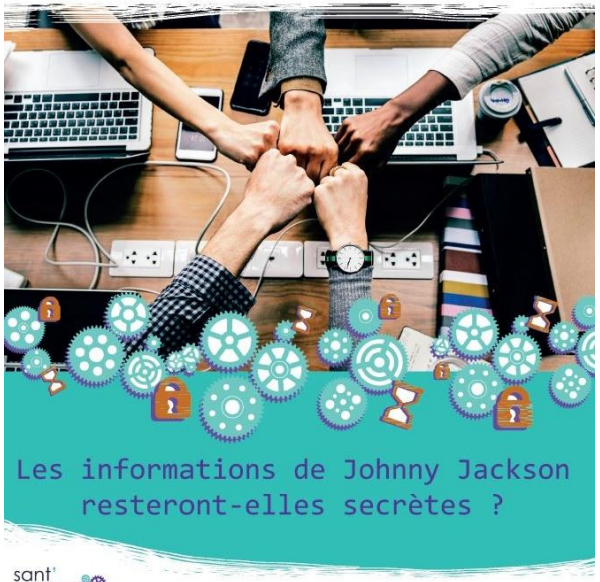
- 5 visuels déclinés en badges et stickers

- Affiches de sensibilisation (différents formats disponibles)
  - Cartes postales
  - Fond d'écran

[Lien pour consulter puis télécharger les affiches]

- Datablockers, protège carte, …
- Vidéos de sensibilisation sur 5 thématiques différentes.

SENSIBILISER
Via le jeu



Défi à relever en 45 minutes, pas une de plus !

Les participants à l'escape doivent se mettre dans la peau de personnages imaginaires : 5 journalistes peu scrupuleux d'un magazine People qui doivent décrocher un scoop sur l'état de santé d'une célébrité pour sauver leur journal de la faillite.

Les bonnes pratiques de base en matière de sécurité numérique ont-elles été bien suivies dans la structure ou seront-elles la clé d'accès aux informations de santé pour les journalistes ?

- Une méthode de sensibilisation innovante, ludique qui implique les apprenants ;
- Ne nécessite aucune connaissance technique particulière, s'adresse à tous publics ;
- Des participants qui doivent se mettre dans la peau "des méchants" et exploiter les mauvaises pratiques ;
- Un scénario contextualisé au secteur santé ;
- Une durée de jeu de 45 min pour ne pas mobiliser les professionnels plus d'1h (briefing / débriefing inclus) ;
- Une formation et un kit de ressources permettant aux structures ligériennes d'être autonomes dans la mise en œuvre.

1850 participants en PDL

Des actions valorisables dans le cadre de l'évaluation de la qualité des ESSMS

Thématique – Démarche qualité et gestion des risques

Critère 3.14 – L'ESSMS est doté d'un plan de gestion de crise et de continuité de l'activité

- **3.14.1 – L'ESSMS définit, avec les professionnels, un plan de gestion de crise et de continuité de l'activité et le réactualise régulièrement**
- **3.14.2 – L'ESSMS communique son plan de gestion de crise en interne et en externe**
- 3.14.3 – Les professionnels participent aux exercices et aux retours d'expérience partagés, organisés par l'ESSMS
- 3.14.4 – Les professionnels sont régulièrement sensibilisés et/ou formés à la gestion de crise

Les cotations étoile

Les cotations étoile permettent aux évaluateurs indépendants de signaler qu'un élément d'évaluation va au-delà des attendus du manuel (pratiques innovantes, acteurs de référence dans un domaine…). L'objectif de cette mention étoile vise à valoriser le travail des professionnels et à identifier les pratiques remarquables afin d'en permettre la diffusion.

Un de nos adhérents qui **a bénéficié de l'ensemble des accompagnements** disponibles a pu **les valoriser** lors de sa visite d'évaluation de la qualité HAS et a obtenu une cotation **« étoile »** pour le critère 3.14

La Sécurité Numérique en Pays de la Loire

Montée en compétence des acteurs de santé des PdL

Formations

Webinaires et ateliers techniques

Base documentaire régionale (Résana)

Stratégie de continuité et reprise d'activité / Préparation à la crise d'origine cyber

Soutien à la réalisation d'exercices de crise cyber (ES)

Accompagnement à l'appropriation de la démarche PCRA

Appui à la gestion des incidents

Messagerie de secours

Animation

Journées régionales (plénière, atelier, stand, …)

Information et communication (Newsletter, réseaux sociaux, …)

Evènements

Sensibilisation

e-learning / faux-phishing

Ateliers présentiels et distanciels

Sant'escape – Sécurité numérique

Vidéos

Evènements

Outils

Affiches / Fonds d'écran / Tapis de souris

Badges métalliques / Stickers

Datablockers

Protège cartes

Accompagnements spécifiques des ESSMS

Exercice de crise d'origine cyber (ESMS)

Centre de ressources SSI mutualisées à destination des ESMS

Appui au Collectif SI MS

Webinaires Fédérations

Accompagnements spécifiques des Libéraux

E-learning / faux-phishing

Ateliers présentiels / distanciels

Outil(s)

Diagnostic cyber (MSP)

Exercice de crise d'origine cyber (MSP)

Cofinancé par l'Union européenne

RÉGION PAYS DE LA LOIRE

Annexes

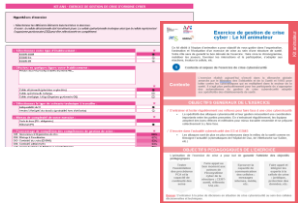
Où retrouver la documentation ?

Page Cybersécurité pour le médico-social

Cycle de webinaires dédiés au médico-social

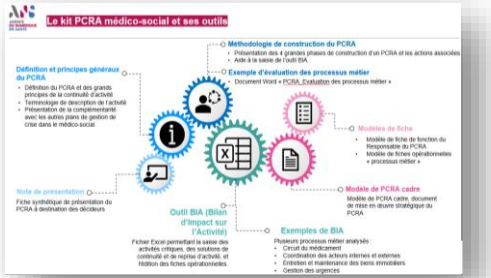
Guide cybersécurité en 13 questions

Kits Exercices de crise



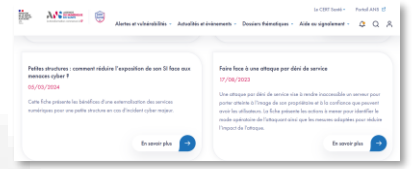
Pourquoi réaliser un exercice de crise ? RETEX de la Ligue Havraise

Le kit PCRA pour le médico-social



Modules sur la thématique cyber

Fiches thématiques – portail cyberveille



Offre de service des CRRC

L'OPSSIMS – Observatoire Permanent de la Sécurité des Systèmes d'Information dans le Médico-Social

AGENCE DU NUMÉRIQUE EN SANTÉ

LE VILLAGE DE LA E-SANTÉ

Pour plus d'information retrouvez nous sur esante.gouv