Exercice de gestion de crise numérique

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

Livret de stimuli

Titre du document

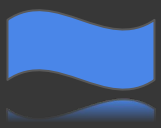
Date	01/02/2021 (date de dernière modification)
Version	202102-0.1 (YYYYMM-VV ou VV est le numéro de la dernière révision du document)
Classification	C2 - Restreint (voir notes ci-dessous pour les différents niveaux de classification)
Diffusion	Direction, chefs de projets concernés, partenaires concernés

Cycle de vie du document

Date	Révision	Rédacteur	Note
01/02/2021	0.1	**Prénom Nom**	Création du document

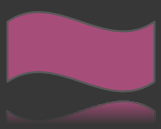
Légende

Stimuli généraux : applicables à l'ensemble des établissements de tous types et obligatoires pour un déroulement cohérent de l'exercice



Stimuli type CH / Clinique

Stimuli type HAD / SSR



Stimuli facultatif

Stimulus n°1

De		*À*
Accueil de la structure de santé		Admin sys. & réseau Support IT Responsable GAM

Préalables au stimulus

Même s'il s'agit d'un soucis mineur qui ne justifie pas le déclenchement de la cellule de crise, la mobilisation de la cellule n'est pas testée. La cellule est donc déjà réunie en amont.

Contenu de l'appel

Attitude : neutre

Bonjour,

Je suis à l'accueil de la structure.

Je vous appelle car je n'arrive plus à accéder à mes dossiers de travail depuis mon poste. Je clique dessus mais il ne se passe rien.

J'ai l'impression que mes applications et notamment le logiciel GAM (Gestionnaire Administratif du Malade) ne sont plus accessibles non plus. J'ai demandé de l'aide à mes collègues mais ils ne comprennent pas non plus d'où peut venir le problème.

Que dois-je faire ?

Réactions attendues

Vérification de l'information / demande de précisions
Aide utilisateur

Stimulus n°2

De	À
Pharmacien	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

X

Contenu de l'appel

Attitude : agacée

Bonjour,

Je travaille au service pharmacie

Nous avons un problème généralisé sur les postes du service de préparation en pharmacie.

Plusieurs des écrans des PC du service sont devenus noirs avec un message en anglais. Mes collègues ont besoin d'accéder rapidement au logiciel pour continuer à saisir les données des patients. Ils se connectent donc sur mon poste en attendant...

Pouvez-vous faire remonter le problème à quelqu'un ? Nous ne pouvons pas continuer à travailler sur un seul poste.

Merci

Réactions attendues

Clarification du problème et actions à mener
Définition des rôles de chacun dans la cellule
Ouverture d'une main courante
Signalement/échange avec les membres de la DSI et CME
Transmettre les informations au service technique qui pourra demander à la DSI si des investigations/actions sont en cours sur les postes problématiques
Ne pas éteindre les PC (les débrancher du réseaux)

Stimulus n°3

De	À
Équipe IT	RSI / RSSI

Préalables au stimulus

X

Contenu de l'appel

Attitude : neutre

Bonjour,

Je fais partie du support IT.

Je vous appelle car l'équipe technique reçoit plusieurs signalements depuis ce matin nous alertant de la difficulté à accéder aux ordinateurs de plusieurs services. D'après les témoignages et les photos reçues, une demande de rançon apparait sur les postes indisponibles.

Êtes-vous au courant de cette situation ? Les appels se multiplient et nous ne pouvons pas fournir plus d'informations au personnel de l'établissement.

Optionnel : *proposer la photo des postes compromis*

Réactions attendues

Qualification de l'incident comme majeur
Transmission de l'alerte à la direction et demander les consignes concernant la demande de rançon
Préparation d'une stratégie de communication notamment pour prévenir le personnel qu'un incident est en cours

Stimulus n°4

De	À
Équipe IT	RSI / RSSI

Contenu du mail

OBJET : [EXERCICE DE CRISE] Informations complémentaires poste compromis

Bonjour,

Suite à mon appel, vous trouverez ci-joint la photo du poste compromis. L'auteur de l'attaque nous indique de rentrer en contact avec lui pour connaitre les modalités de paiement pour obtenir la clé de déchiffrement et éviter une publication des données patients.

De mon côté, je continue à recevoir des appels, avez-vous des directives à me donner sur les actions à mener ? Que puis-je dire aux interlocuteurs qui me demandent plus d'information ?

Dans l'attente de votre retour,

Le service IT

Réactions attendues

Communication et partage d'information entre la DSI et la direction
Anticipation des impacts sur les services/personnels/patients
Faire un point avec le support IT pour partager les consignes de communication à destination du personnel
Déclaration sur le portail des incidents ou contact du CERT-Santé

Stimulus n°4 bis

De	À
Équipe IT	RSI / RSSI

Contenu de l'appel

Attitude : Neutre

Bonjour, ici le service informatique

Je souhaitais vous tenir au courant de l'état d'avancement des investigations en cours.

Une grande partie du parc informatique est touché ainsi que plusieurs serveurs de bases de données et d'applications.

On continue à investiguer mais je voulais vous tenir au courant au fur et à mesure de l' évolution de la situation.

Merci

Réactions attendues

Communication et partage d'information entre la DSI et la direction
Anticipation des impacts sur les services/personnels/patients
Faire un point avec le support IT pour partager les consignes de communication à destination du personnel
Déclaration sur le portail des incidents ou contact du CERT-Santé

Stimulus n°5

De	À
Personnel de l'accueil	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

Ce stimulus doit être envoyé si la cellule n'a pas déclenché le mode dégradé. Il peut également être envoyé si vous souhaitez expliquer le mode dégradé.

Contenu de l'appel

Attitude : neutre / légèrement inquiète sur le fonctionnement

Bonjour,

Je suis à l'accueil de la structure.

Je dois enregistrer un nouveau patient mais n'ayant plus accès à nos ordinateurs, je ne sais pas comment faire.
De même, nous n'avons plus accès aux plannings et nous ne savons pas comment orienter les patients qui se présentent pour leurs séances de (...).

Comment doit-on faire sans ordinateurs ?

Merci

Réactions attendues

Réflexion sur l'existence ou non de moyens dégradés pour continuer à travailler
Explication du mode dégradé
Rassurer la personne sur l'utilisation de ce mode
Répondre aux questions potentielles

Stimulus n°6

De	À
ARS	DSI/RSSI

Préalables au stimulus

Ce stimulus doit être envoyé si la cellule n'a pas fait de de notification auprès de l'ANSSI, du CERT-santé

Contenu de l'appel

Attitude : neutre / à l'écoute

Bonjour,

Je suis membre de l'ARS

Nous avons été notifié qu'un incident de cybersécurité était en cours dans votre établissement.
Je voulais m'assurer que toutes les mesures avaient été mises en place pour la prise en charge de celui-ci.

Par ailleurs, le CERT-santé a-t-il été notifié ?

Merci

Réactions attendues

Notification auprès de l'ANSSI et/ou du CERT-Santé

Stimulus n°7

De	À
Chirurgien	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

Ce stimulus peut être envoyé si l'ensemble des services n'ont pas été prévenu du passage en mode dégradé

Contenu de l'appel

Attitude : Agacé/pressé

Bonjour,

Je suis chirurgien.

Je vous contacte parce que j'ai un besoin urgent d'accéder aux radios de l'un de mes patients. Celles-ci ont normalement été versées au dossier du patient avant la coupure.

Y a-t-il un endroit ou je peux trouver la dernière version du plan de soins des patients ? J'ai l'impression que les documents auxquels j'ai accès remontent à plusieurs jours.

Merci

Réactions attendues

Explication du mode dégradé
Explication sur l'emplacement des documents
A la suite de ce stimulus, la cellule de crise doit prendre conscience de l'importance de réaliser l'appel à tous les services pour expliquer la situation.
Répertorier l'ensemble des services pour montrer la réalité du terrain et le temps que doit passer le personnel à rassurer/expliquer la situation.

Stimulus n°8

De	À
RSSI GHT / DSI Groupe	RSSI/Direction

Préalables au stimulus

Ce stimulus doit être adapté au fonctionnement de votre structure. Il peut être envoyé si votre cellule n'a pas pensé à l'aide que peut apporter le RSSI GHT ou la DSI Groupe.

Contenu de l'appel

Bonjour,

Je suis le RSSI du GHT (...) / je fais parti de la DSI du groupe (...)

Je vous appelle au sujet de l'incident de sécurité en cours dans votre établissement.

Avez-vous déclarer l'incident aux autorités via la chaîne de signalement ?

Avez vous besoin d'aide ?
Pouvez vous me décrire le type d'aide nécessaire (matériels, humains…)?

Réactions attendues

Réflexion sur le type d'aide qui peut être apporté
Identification des besoins matériels et humains à ce stade de la crise
Anticipation des besoins si la crise dure

Stimulus n°9

De	À
Responsable de service	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

Stimulus à envoyer si la cellule de crise n'a pas déclenché le mode dégradé

Contenu de l'appel

Bonjour,

Je suis responsable de service

Je vous contacte parce que mes infirmiers ne peuvent plus accéder aux logiciels pour valider l'administration des traitements de plusieurs patients. J'ai l'impression que nous avons perdu la main sur toutes nos données.

J'ai deux patients en attente de leur séance thérapeutique.

D'ailleurs, j'entends dire de la part du service administratif que l'on ne peut plus créer de fiches d'admissions de nouveaux.
patients
Comment puis-je accéder aux informations pour continuer à soigner mes patients ?

Merci

Réactions attendues

X

Stimulus n°10

De	À
CERT-Santé	DSI/RSSI

Préalables au stimulus

Stimulus a envoyer 10 minutes environ après l'appel au CERT-Santé. Il peut se faire par mail ou par téléphone (n'énoncer que ce qui est en gras)

Contenu du mail/appel

OBJET : [EXERCICE DE CRISE] Signalement n°RM#435653

Bonjour,
Nous avons bien pris en compte votre signalement, enregistré sous la référence [RM#435653].
Dans le cadre de notre procédure de traitement d'incident, nous souhaiterions obtenir davantage d'informations. Vous trouverez ci-après
les éléments demandés ainsi que des premières recommandations.

- **Nom et Prénom / Courriel / Numéro de téléphone du RSSI et/ou de la personne en charge de cet incident**
- **Quelles sont les machines concernées par l'infection ? Quels types de fichiers ont été chiffrés ? Le SI compromis est-il en lien avec d'autres SI ?**
- **Quel est l'impact de cet incident sur la poursuite de vos activités ?**
- **Date et heure de l'infection**
- Connaissez-vous le vecteur de la compromission (courriel malveillant, exploitation de vulnérabilité, compromission de SI, etc.) ?
- Connaissez-vous le rançongiciel ? Sa version ?
- Quelle est l'extension des fichiers chiffrés ?
- Avez-vous des empreintes numériques (MD5, SHA1, SHA256 ...), une souche du rançongiciel ou des captures d'écran à nous transmettre ?
- Pouvez-vous communiquer la demande de rançon, les adresses courriel impliquées, les portefeuilles de Bitcoin ?
- **Avez-vous des sauvegardes saines qui permettent de restaurer le ou les systèmes infectés ?**
- Avez-vous engagé un prestataire pour vous aider à remédier à cette attaque ? Si oui, lequel ? Quelles ont été les mesures réactives prises à la suite de cet incident ?
- Dans le cas où des données à caractère personnel aient été impactées, avez-vous déclaré l'incident à la CNIL ?

Stimulus n°10 (suite)

De	À
CERT-Santé	DSI/RSSI

Contenu du mail/appel

[SUITE]

• Envisagez-vous ou avez-vous déjà effectué un dépôt de plainte ?
• Il est très peu probable que les données puissent être déchiffrées. Toutefois, sollicitez-vous une assistance du CERT-Santé dans vos actions de remédiation ? Si oui, pour quel(s) champs d'intervention ?

Dans l'optique d'une démarche pénale (recommandée), nous vous rappelons que vous êtes invité à conserver sans y apporter de modification, tout document ou information établissant les faits et qui constituent potentiellement des éléments de preuve :
- copies physiques des disques durs (ou VM) des postes compromis ;
- copies des journaux d'événements disponibles sur tout équipement réseau qui auraient pu permettre la transmission des codes malveillants.

Enfin, selon le type et la version du rançongiciel, il est possible qu'il existe un outil ou des clés de déchiffrement dédiés. Un référentiel de ces solutions est disponible sur le site Internet No More Ransom (https://www.nomoreransom.org/fr/index.html). Nous vous invitons à consulter les conseils préalables et guides d'utilisation avant toute opération de déchiffrement.

Nous vous demandons de bien vouloir nous tenir informés de l'évolution de la situation et revenons vers vous rapidement pour effectuer de premières investigations.

Cordialement,

CERT-Santé

Réactions attendues

Réflexion sur l'anticipation d'un dépôt de plainte
Réflexion sur l'impact d'une potentielle fuite de données (prévenir la CNIL)

Stimulus n°11

De	À
ANSSI	DSI/RSSI

Préalables au stimulus

Ce stimulus peut être envoyé si vous disposez d'une GTC au sein de votre structure.

Contenu de l'appel

Bonjour,

Je fais partie du service investigation de l'ANSSI.

Nous travaillons sur votre incident en cours et nous souhaitons vous signaler que nous avons interceptés des messages entre hackers indiquant qu'ils revendaient des accès à la GTC (gestion technique centralisée) de votre structure.

Savez vous qu'implique une coupure de votre GTC ? Des personnes peuvent-elles être en danger si la détection incendie est neutralisée par exemple ?

Merci

Réactions attendues

Réflexion sur une criticité maximale
Anticipation impacts patients et personnels
Réflexion sur une stratégie de communication

Stimulus n°12

De	À
Membre du service RH	DPO/RSSI/Direction

Préalables au stimulus

Ce stimulus doit être envoyé si aucune communication interne n'a été réalisée envers les membres administratifs

Contenu de l'appel

Bonjour,

Je suis membre du service RH.

Suite à l'incident actuellement en cours dans notre structure, je souhaitais savoir ce que la direction avait prévu de faire concernant la demande de rançon.

Est-ce que l'établissement a prévu de payer la rançon ?

Est-ce que des données ont fuité ?

Merci

Réactions attendues

Communication interne auprès de l'ensemble des services administratifs si cela n'a pas été déjà réalisé.
Actions sur une potentielle fuite de donnée.

Stimulus n°13

De	À
DPO ARS	DPO/RSSI/Directeur

Préalables au stimulus

X

Contenu de l'appel

Attitude : neutre

Bonjour,

Je suis déléguée à la protection des données de l'ARS.

Je souhaitais faire un point de situation de l'incident en cours au sein de votre établissement.

Pouvez-vous me dire si une fuite de données est suspectée ? Quelles données peuvent potentiellement avoir été compromises par l'attaque ?

Merci

Réactions attendues

Définition du périmètre de l'attaque et des actifs touchés si ça n'a pas encore été fait.
Recontacter le CERT-Santé pour obtenir plus d'information
Début de réflexion sur une potentielle fuite de donnée et de contact de la CNIL

Stimulus n°14

De	À
CERT-Santé	DSI/RSSI

Préalables au stimulus

X

Contenu de l'appel

Bonjour,

Ici le CERT-Santé.

A priori, des postes clients et serveurs ont été compromis par un rançongiciel.

Par ailleurs, nous en savons plus sur l'origine de l'attaque qui aurait débuté sur le poste « accueil », très certainement à la suite de l'insertion d'une clé USB infectée il y a quelques jours.

Nous essayons d'identifier le programme malveillant ainsi que son mode opératoire.

Nous reviendrons vers vous dès que nous aurons plus d'information.

Réactions attendues

Tenir à jour la main courante

Stimulus n°15

De	À
Groupe de hackers	Direction

Préalables au stimulus

L'envoi de ce stimulus suppose au préalable l'envoi du stimulus n°11.

Contenu du mail

OBJET : [EXERCICE DE CRISE] Patients en danger

Nous avons obtenu le contrôle sur votre système de gestion technique centralisé

Ne tentez aucune action sur ces dispositifs sinon nous serons contraints de désenclencher vos alarmes incendies et déclencher un incendie dans votre établissement.

Vos patients sont en danger.

Pour éliminer ce risque et vous redonner le contrôle sur votre structure nous vous demandons de payer 50 bitcoins sous 48h.

Réactions attendues

Ne pas céder à la panique
Faire vérifier le périmètre de la GTC
Débuter une communication interne et externe
Débuter les démarches pour un dépôt de plainte

Stimulus n°16

De	*À*
Technicien de laboratoire	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

X

Contenu de l'appel

Attitude : agacée

Bonjour,

Je suis technicien en laboratoire.

Avec la coupure réseau et le nombre de prélèvements à analyser, nous ne parvenons plus à faire parvenir les résultats des patients dans un temps raisonnable.

Quelle solution avons-nous ?

Merci

Réactions attendues

Réflexion sur l'augmentation des effectifs

Stimulus n°17

De	À
Personnel d'accueil	Responsable communication / Direction

Préalables au stimulus

X

Contenu de l'appel

Attitude : agacée

Bonjour,

Je suis à l'accueil de la structure.

Je vous informe que certains patients se sont plaints de la lenteur et de la désorganisation dans certains services.

La presse locale commence à nous contacter pour savoir ce qu'il se passe. Des messages mentionnant l'hôpital commencent aussi à arriver sur les réseaux sociaux.

Que dois-je dire aux patients ? à leurs familles ? on me pose des questions ? Que dois-je répondre ?

Merci

Réactions attendues

Débuter la réflexion sur la stratégie de communication externe et la définition d'éléments de langage.
Partage d'information avec la direction sur la stratégie de communication
Rassurer le personnel d'accueil

Stimulus n°18

De	À
CERT-Santé	DSI/RSSI

Contenu de l'appel

Attitude : neutre

Bonjour,

Ici le CERT-Santé.

Nous avons obtenu les résultats des dernières investigations.

Le rançongiciel Ragnarok est bien à l'origine du dysfonctionnement que nous observons sur les postes.

Suite à l'insertion d'une clé USB, l'attaquant aurait obtenu des droits d'administrateur sur le poste accueil en lançant des outils de récupération d'identifiants Windows sur ce poste. Il aurait alors exploité la vulnérabilité MS17-010 datant d'octobre 2017 pour obtenir des droits d'administrateur sur le serveur de gestion des DPI. Le chiffrement des données aurait alors commencé. L'attaquant aurait réussi à compromettre d'autres postes pour diffuser le rançongiciel.

Des investigations sont encore en cours pour savoir s'il y a réellement eu une fuite de données.

Réactions attendues

Informer la direction des nouvelles informations obtenues
Faire remonter la nécessité de mettre à jour les serveurs
Mobilisation de techniciens informatiques sur les postes infectés
Faire une notification auprès de la CNIL ou réadapter celle qui a été réalisée auparavant

Stimulus n°19

De	À
EHPAD	Direction

Préalables au stimulus

Ce stimulus peut être envoyé si votre établissement est en lien ou à proximité d'un autre établissement. Il doit être adapté à la situation.

Contenu de l'appel

Attitude : affolée

Bonjour,

Ici l'EHPAD X

Nous venons de recevoir des menaces par mail nous indiquant que la GTC avait été neutralisée, que les alarmes incendies avaient été désactivée et des menaces incendies.

Comment doit-on procéder pour l'évacuation des patients ? Est-ce que l'on doit appeler la police ?

Est-ce que l'on doit transférer les patients dans un autres établissement ? Comment on doit organiser ce transfert, nous n'avons pas assez de personnel ni de moyen de transport !

Le personnel de l'EHPAD est très tendu, quelles instructions dois-je leur donner ?

Réactions attendues

Redéfinir le périmètre de l'attaque et des actifs touchés
Définir les impacts d'une seconde structure liée à l'établissement qui serait touché.

Stimulus n°20

De	À
Médecin externe	Direction

Préalables au stimulus

X

Contenu de l'appel

Attitude : étonné/mécontent

Bonjour,

Je suis le médecin de plusieurs de vos patients

Je souhaitais accéder à la situation de mes patients mais mon application ne fonctionne pas. Ou puis je trouver les informations mises à jour liées à mes patients ?

Par ailleurs, un patient m'a interrogé sur le monitoring à distance de ses appareils, sait-on si les données peuvent toujours être suivies par les médecins ?

Merci

Réactions attendues

Vérifier la bonne application des procédures dégradées

Stimulus n°21

De	À
Cadre de santé	RH/DRH/Direction

Préalables au stimulus

Ce stimulus doit être adapté au fonctionnement de la structure.

Contenu de l'appel

Attitude : agacée/fatiguée

Bonjour,

Je suis cadre de santé.

Mon service s'inquiète de l'organisation des équipes dans les prochains jours, si la crise dure. A-t-on une visibilité sur une possible réorganisation des équipes et des astreintes ?

Mes équipes se plaignent car elles auraient déjà dû faire leur rotation depuis un moment.

Merci

Réactions attendues

Stimulus n°22

De	À
Patient	Médecin

Préalables au stimulus

x

Contenu de l'appel

Attitude : inquiet

Bonjour,

Je vous appelle parce que je suis un ancien patient de votre structure et je viens de recevoir une facture de votre part par email.

Ca me paraît bizarre parce que tous mes frais devaient être pris en charge. Je voulais être certain que vous êtes bien l'auteur de cette facturation.

En fonction de la réponse de l'interlocuteur : Comment se fait-il que je reçoive ce type de mail ? J'ai entendu dire que vous aviez une cyberattaque est-ce que je dois m'inquiéter que mes données aient peut-être fuité ?

Merci

Réactions attendues

Vérifier la fiabilité de l'information
Demander une copie d'écran du mail en question
Rassurer le patient - être précis dans les réponses apportées à l'interlocuteur
Réflexion sur une possible fuite de données - ne pas se précipiter

Stimulus n°23

De	À
Annabelle Journeaux (journaliste de France 3)	Responsable communication / Direction

Préalables au stimulus

Ce stimulus doit être envoyé de façon insistante comme le ferait un véritable journaliste. Il ne faudra pas laisser l'interlocuteur raccrocher trop rapidement.

Contenu de l'appel

Attitude : insistante

Bonjour,

Je suis Annabelle Journaux, journaliste chez France 3.

Nous souhaitons communiquer sur la cyberattaque qui a touché votre structure. Plusieurs informations m'ont déjà été communiquées mais j'aimerais les compléter avec des témoignages notamment pour connaître l'origine de l'incident.

Puis-je rencontrer le responsable de la structure pour en discuter ?

Réactions attendues

Ne pas mentir.
Réaliser une veille sur les réseaux sociaux et voir comment la journaliste a obtenu ces informations
Préparer un communiqué de presse en lien avec les équipes communications et la CNIL

Stimulus n°24

De	À
Annabelle Journeaux (journaliste de France 3)	Responsable communication / Direction

Préalables au stimulus

Ce stimulus peut être envoyé quelques minutes après l'appel de la journaliste.

Contenu du mail

OBJET : [EXERCICE DE CRISE] Article France 3

Bonjour,

Comme convenu vous trouverez ci-joint l'article de presse que nous allons publier sur le site internet de France 3 ce jour.

Bien cordialement,

Annabelle Journaux,
Journaliste chez France 3

CYBERATTAQUE DE GRANDE AMPLEUR A (nom de l'établissement) : LE SERVICE DE SOIN PARALYSÉ

L'établissement … a été frappé par une cyberattaque de grande ampleur ce matin: "Les services sont totalement désorganisés, nous avons dû attendre 5h avant que mon époux soit admis" nous raconte Geneviève qui a pu constater les conséquences de la cyberattaque au sein de l'établissement de santé.

Plusieurs témoins nous rapportent qu'un rançongiciel – programme malveillant qui provoque le chiffrement de tout ou partie des données d'un ordinateur - serait à l'origine de l'attaque et que plusieurs services seraient à l'arrêt pour une durée indéterminée.

L'établissement n'a pas encore souhaité s'exprimer pour confirmer les faits. Nous attendons une prise de parole dans la journée.

Stimulus n°25

De	À
Service restauration	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

Ce stimulus doit être personnalisé en fonction des processus instaurés dans votre établissement.

Contenu de l'appel

Attitude : inquiet

Bonjour,

Je fais partie du service restauration

Je dois réaliser la commande des plateaux repas pour l'ensemble des patients de la structure mais je n'ai pas accès à mon PC pour passer les commandes.

De plus, sans mon PC, je n'ai pas accès aux régimes alimentaires spécifiques des patients et leurs allergies.

Que dois-je faire pour les jours avenirs ?

Merci

Réactions attendues

Identification organisation dégradée et pilotage

Stimulus n°26

De	À
Famille de patient	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

X

Contenu de l'appel

Attitude : inquiète

Bonjour,

Je suis la fille de l'un de vos patients

Je viens de voir sur internet que (Nom d'établissement) était victime d'une cyberattaque. Ma mère fait partie de vos patients et son infirmière est en retard pour ses soins. Est-ce que ce retard est lié à l'attaque en cours ?

Je suis dans une autre région, je n'ai personne pour s'occuper de ma mère. Est-ce que l'infirmière va bien venir chez ma mère pour ses soins ?

Je suis assez inquiète si vous commencez déjà à avoir des soucis de personnels .. Qui va prendre en charge les soins de ma mère sur ces prochains jours ?

Merci

Réactions attendues

Rassurer l'interlocuteur - prendre les informations concernant le patient
Ne pas répondre aux questions sur la crise

Stimulus n°27

De	À
Personnel d'accueil	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

X

Contenu de l'appel

Attitude : agacée/fatiguée

Bonjour,

Je travaille à l'accueil de la structure

J'ai reçu des appels de patients et de leurs familles qui sont inquiets d'une possible fuite de données suite à l'incident qui touche la structure.

Certains m'ont indiqué avoir reçu un mail sur leur adresse mail personnelle, des menaces de divulgation de leurs données personnelles si l'établissement ne paie pas la rançon.

Je suis actuellement avec des familles de patients à l'accueil qui me posent des questions sur les démarches à suivre. Est-ce que l'établissement va payer pour éviter que ces données ne soient diffusées ?

Est ce que ces patients et familles doivent aller porter plainte suite à ces menaces par mail ?

Réactions attendues

Contact avec la CNIL pour une remontée d'information
Prévoir du personnel d'information sur place si possible
Préparation d'un communiqué

Stimulus n°28

De	À
Pharmacien	Directeur des soins Cadre de santé Responsable de pôle

Préalables au stimulus

Ce stimulus doit être personnalisé en fonction des processus instaurés dans votre établissement.

Contenu de l'appel

Attitude : affolée

Bonjour,

Je suis l'adjoint du responsable de la pharmacie.

Nous venons de nous rendre compte que nous avons interverti le traitement de deux patients par erreur malgré la double vérification imposée.

Nous n'arrivons plus à gérer le mode papier car nous craignons que d'autres erreurs soient réalisées.

Que devons nous faire pour ces patients ? Doit-on les avertir de cette erreur ?

Quelle organisation pouvons-nous mettre en place pour éviter de nouvelles erreurs ?

Merci

Réactions attendues

Prendre les mesures nécessaires en fonction des processus internes
Prévoit éventuellement si possible du personnel en plus ou un roulement

Stimulus n°29

De	À
Syndicat	RH/DRH/Direction

Préalables au stimulus

x

Contenu de l'appel

Attitude : insistant

Bonjour,

Je suis le représentant de la CGT

Suite à l'incident en cours au sein de la structure, nous souhaitons démarrer de nouvelles négociations en faveurs du personnel.

Les salariés subissent de plein fouet l'inflation mais également l'épuisement dû à cette cyberattaque.

Nous souhaitons donc organiser dans les plus brefs délais, sans attendre les échéances habituelles des négociations annuelles, une réunion de négociation relative aux salaires, congés et à la politique salariale.

Merci

Réactions attendues

Stimulus n°30

De	À
Gestionnaire de paie	RH/DRH/Direction

Préalables au stimulus

Stimulus facultatif : à voir si votre système de paie est externalisé ou non

Contenu de l'appel

Attitude :

Bonjour,

Je suis la gestionnaire de paie de la structure

Suites aux dysfonctionnement des outils numériques, et la fin du mois approchant, je ne sais pas vraiment comment réaliser la paie ?

Je crains la réaction des représentants du personnel.

Réactions attendues

Trouver une solution alternative pour la gestion des paiements des salaires
Effectuer en amont une communication interne à ce sujet

Stimulus n°31

De	À
Syndicat	RH/DRH/Direction

Préalables au stimulus

L'envoi de ce stimulus suppose au préalable l'envoi du stimulus n°29.

Contenu du mail

Madame, Monsieur,

Par la présente et conformément à l'article L2511-1, L2512-1 et suivants du Code du travail, nous avons l'honneur de déposer un préavis de grève.

Notre mouvement de protestation commencera le ../../… à 9h et se terminera le ../../….
Par l'intermédiaire de ce mouvement, nous voulons attirer votre attention sur ces faits :

- Le sous effectif entraîné par la cyberattaque
- L'inquiétude due à la possible fuite de données
- L'inquiétude due au possible non versement des salaires

A ce titre nous revendiquons ces éléments:

- Revoir la politique salariale
- Une communication transparente concernant les fuites de données des salariés
- L'engagement de la direction sur le versement des salaires
- L'engagement de la direction sur augmentation des temps de repos compensateurs ou RTT

Réactions attendues

Stimulus n°32

De	À
PC Sécurité	RH/DRH/Direction

Préalables au stimulus

X

Contenu de l'appel

Attitude : Neutre/Demande d'informations

Bonjour,

Ici le PC sécurité

Nous vous informons qu'un incident de sécurité est survenu il y a quelques minutes à l'accueil de la structure.

Un homme âgé d'une quarantaine d'année s'est énervé et a commencé à être virulent avec la secrétaire d'accueil.

Nous avons été appelé par le personnel pour maîtriser cet individu. Nous l'avons évacuer de la salle d'attente. Il est actuellement avec du personnel de sécurité.

Il semble que la secrétaire d'accueil n'ai pas été blessée, mais elle est très choquée. Doit-on appeler la police et garder l'individu avec nous ?

Pour information, la salle d'attente est relativement tendue.

Réactions attendues

Appel de la police en fonction de la gravité de l'évènement
Prévoir du personnel pour apaiser la salle d'attente

Stimulus n°33

De	À
Louis Feuilleux (Journaliste pour Le Monde)	Responsable communication / Direction

Préalables au stimulus

Ce stimulus doit être envoyé si aucun communiqué de presse n'a été réalisé à la suite du premier stimulus de France 3

Contenu de l'appel

Attitude : insistant

Bonjour,

Je suis Louis Feuilleux, journaliste pour Le Monde.

Nous aimerions tenir informés les habitants de la région de l'évolution l'incident qui a eu lieu ce jour dans votre structure.

Quelles sont les dernières nouvelles ?
Est-ce vrai que vous travaillez sur papier et que vous n'arrivez-plus à soigner correctement les patients ? Des patients sont-ils en danger ?

Quand pensez-vous qu'un retour à la normale pourrait-être envisagé ?

Allez-vous réaliser un communiqué de presse officiel sur la situation?

Réactions attendues

Ne pas répondre en direct aux questions
Préparer un communiqué de presse

Stimulus n°34

De	À
Famille de patient	Responsable communication / Direction

Préalables au stimulus

Ce stimulus doit être personnalisé au contexte de l'établissement

Contenu de l'appel

Attitude : inquiète

Bonjour,

Je suis la compagne de l'un de vos patients.

Je viens de voir à la télé que vous subissez une attaque informatique et que la clinique allait fermer et que vous alliez évacuer les patients.

Malheureusement, je suis en déplacement et je ne peux pas venir chercher mon compagnon. Que dois-je faire ?

Merci

Réactions attendues

Stimulus n°35

De	À
CERT-Santé	DSI/RSSI

Préalables au stimulus

x

Contenu de l'appel

Attitude : neutre

Bonjour,

Ici le CERT-Santé.

Nous sommes en train de mettre en œuvre des moyens connus pour déchiffrer les postes infectés par le rançongiciel.
Il nous faudra quelques heures pour réaliser les correctifs à distance avec l'aide de vos équipes en interne / techniciens.

D'après nos investigations, aucune donnée ne semble avoir fuité.

Réactions attendues

Coordination avec les autorités (la CNIL) sur les messages à faire passer
Communication auprès des collaborateurs pour indiquer que l'origine de l'attaque a été identifiée et qu'un retour à la normale est prévu prochainement

Stimulus n°36

De	À
Coordinateur des transports	Agent logistique

Préalables au stimulus

X

Contenu de l'appel

Bonjour,

Je suis coordinatrice des transports accompagnés

Avec la coupure réseau, je n'ai plus accès au planning des transports personnalisés à prévoir pour que nos patients puissent être emmenés à leurs activités.

Savez-vous s'il existe une sauvegarde de secours des adresses des personnes à transporter ou de leurs numéros de téléphone ?

Réactions attendues

Débuter la réflexion sur les modes dégradés pour assurer la logistique

Stimulus n°37

De	À
Membre de l'équipe IT	Cellule de crise

Préalables au stimulus

Stimulus facultatif : à voir en fonction du fonctionnement de la structure
L'envoi de ce stimulus suppose la venue en directe au sein de la cellule pour le partage d'information

Contenu de l'appel

Bonjour,

Je suis membre de l'équipe informatique

Je viens vous prévenir que la téléphonie interne est HS.

Plusieurs services se sont déplacés pour nous alerter.

Comment fait-on sans téléphone ? Qu'est ce que je dois dire aux équipes ?

Réactions attendues

Solutions alternatives de moyens de communication

Stimulus n°38

De	À
Membre de l'équipe IT	DSI/RSSI

Préalables au stimulus

x

Contenu du mail

Bonjour,

Avec l'aide du CERT-Santé nous avons pu rétablir un accès normal aux postes de travail et aux serveurs locaux.

Les correctifs conseillés par le CERT-Santé vont pouvoir être déployés.
Quel sera le processus pour décontaminer et organiser la reprise du fonctionnement en mode nominal ?

Merci

Réactions attendues

Coordination équipe RSSI et équipes métier
Publication du communiqué de presse
Décision de sortie de crise
Lancer des analyses complémentaires pour s'assurer qu'il n'y aura pas de possibilité de nouvelle attaque (porte dérobée)

Merci