semaine européenne DE LA E-SANTÉ

Contexte & état de la menace cyber

Panorama de la menace cyber

ANSSI

CERT Santé

Tour de table

Présentation des intervenants

Silvère RUELLAN
Chef du bureau cybersécurité santé et affaires sociales

Oliver CROS
Expert cybersécurité & Réponse à incident


KEEP
CALM

Quelques attaques ces derniers jours…

« Les données personnelles d'habitants de Betton divulguées sur internet »

« Le groupe de casinos MGM paralysé par une cyberattaque »

« La Cour pénale internationale victime d'un incident de sécurité »

À qui le tour ?

« L'assurance maladie des Philippines touchée par une cyberattaque »

« La ville de Morlaix victime d'un rançongiciel »

« La fédération néerlandaise de football paye une rançon à un cybergang »

« La chaîne Pizza Hut victime d'une cyberattaque en Australie »

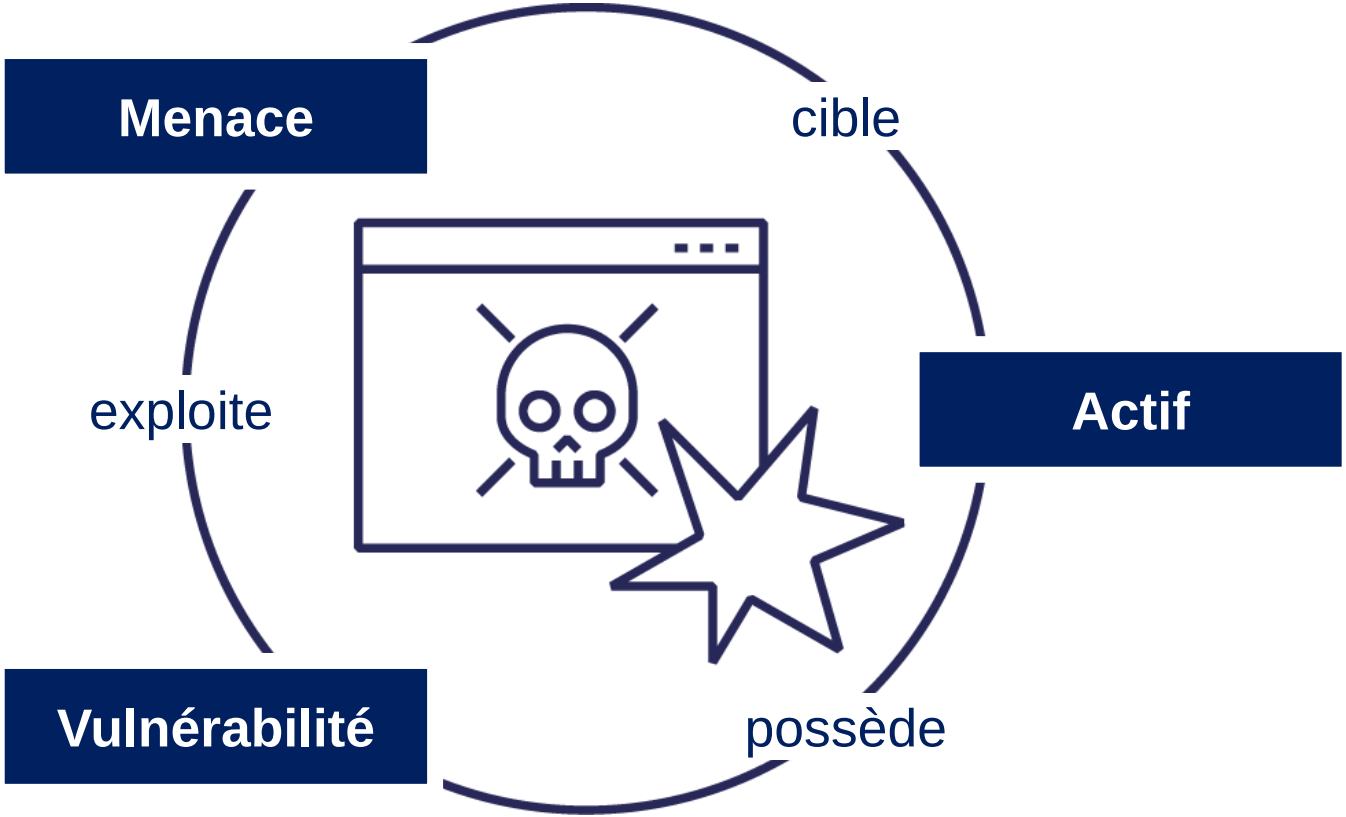
Le secteur santé n’est pas épargné

Quelques attaques marquantes :

- CHU de Rouen (2019)
- CH de Dax (2021)
- CH de Villefranche/Saône (2021)
- GHT Cœur Grand Est (2022)
- CH Sud Francilien (2022)
- CH de Versailles (2022)
- GHT de La Réunion (2023)
- CHU de Brest (2023)
- CHU de Rennes (2023)
- ? (?)

Illustration reproduite avec l’autorisation de Me Ledieu : https://technique-et-droit-du-numerique.fr/retex-de-la-cyber-attaque-contre-le-chu-de-brest-podcast-nolimitsecu-23-juillet-2023

Anatomie d’un incident de sécurité



Les acteurs de la menace

Menace cybercriminelle

- Groupes criminels
- Motivation : l'argent
- Attaques opportunistes, phénomène de masse, professionnalisation
- Rançongiciel, vol et vente de données personnelles

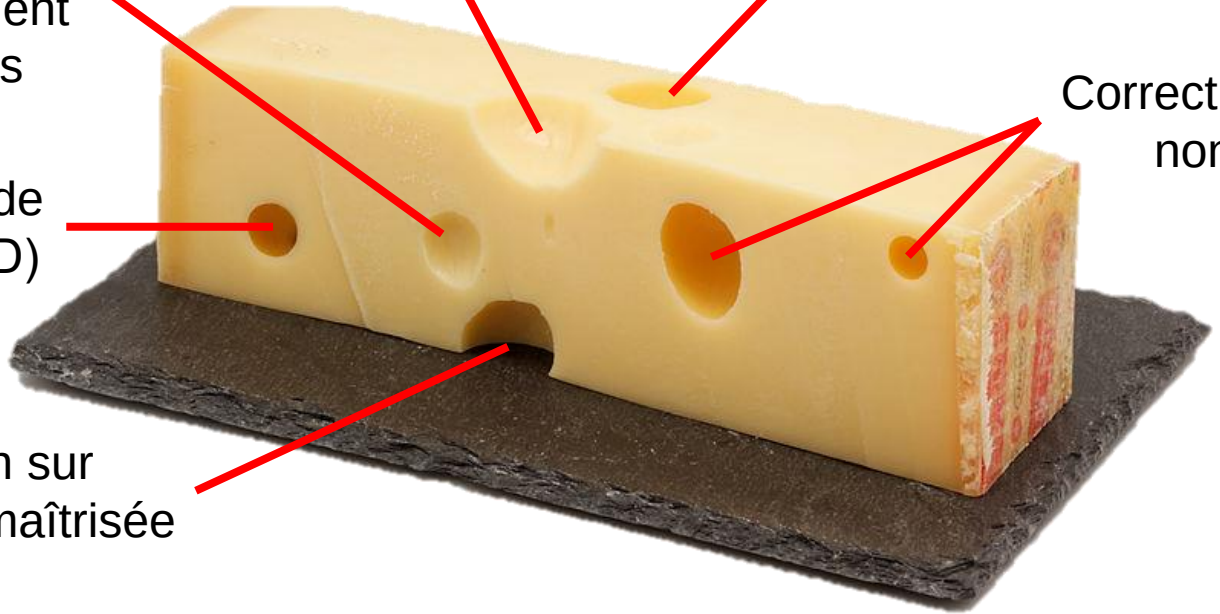
Menace stratégique

- Groupes étatiques ou financés par des États
- Motivation : espionnage, déstabilisation
- Attaques ciblées, furtivité
- Moyens techniques importants
- Espiogiciel, wiper, rançongiciel

Menace isolée

- Individus isolés : hacktivistes, employés mécontents, etc.
- Motivation : idéologie, exploit technique, vengeance, etc.
- Attaques ciblées
- Moyens plus limités
- DDoS, défiguration de site

Les vulnérabilités couramment observées



Sauvegardes inexistantes ou insuffisamment sécurisées

Défaut de supervision

Méthode d'authentification faible

Correctifs de sécurité non installés

Vulnérabilité de l'annuaire (AD)

Exposition sur Internet non maîtrisée

Illustration : https://commons.wikimedia.org/wiki/File:Emmental_(fromage)_01.jpg (licence Creative Commons)

- Une bonne maturité cyber chez certains établissements, **pas de fatalité**

- Lancement du **programme CaRE** par le ministère de la santé, mobilisant tous les acteurs nationaux et locaux

- Changement d'échelle dans la réglementation cyber avec la directive **NIS 2**

Illustration : https://commons.wikimedia.org/wiki/File:We_Can_Do_It!_NARA_535413_-_Restoration_2.jpg (domaine public)

Panorama de la cybermenace 2022

Grands évènements sportifs Évaluation de la menace 2023

Rapports, alertes, IoC, recommandations :

https://www.cert.ssi.gouv.fr

et suivez les publications de l'ANSSI !

Les chiffres du CERT Santé

Gestion des incidents

592
incidents déclarés

165
demandes d'accompagnement

103
interventions d'appui technique

Veille proactive

2200
alertes envoyées

76
cas de compromission

20
Interventions d'assistance

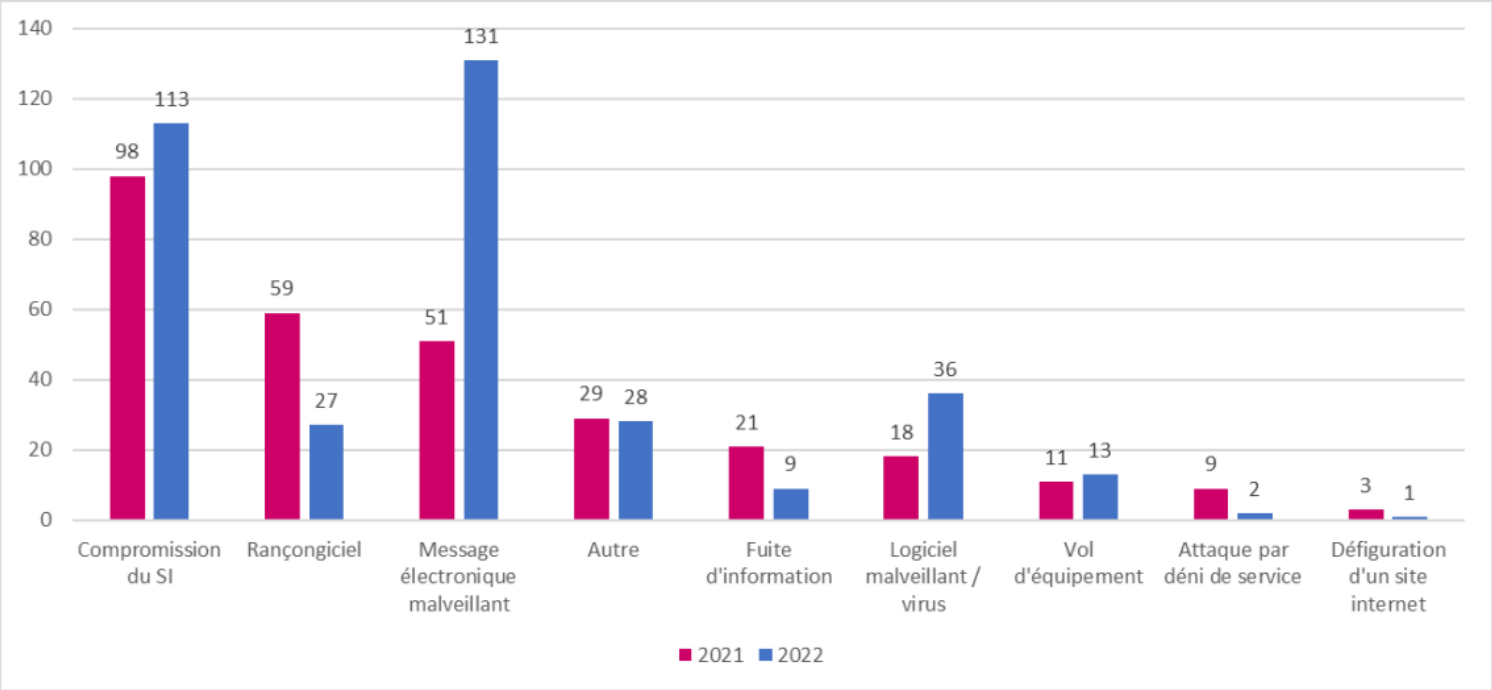
Bulletins & Audits de cybersurveillance

303
Bulletins de veilles partagées

112
audits réalisés

Les grandes tendances du CERT Santé

D'après l'observatoire, l'année 2022 a été marquée par une forte activité malveillante relative **au vol d'identifiants (login – mot de passe) de comptes de messagerie et de comptes d'accès à distance**. Une augmentation significative de la **compromission de comptes de maintenance** des solutions d'infrastructures et applicatives des structures a été observée.

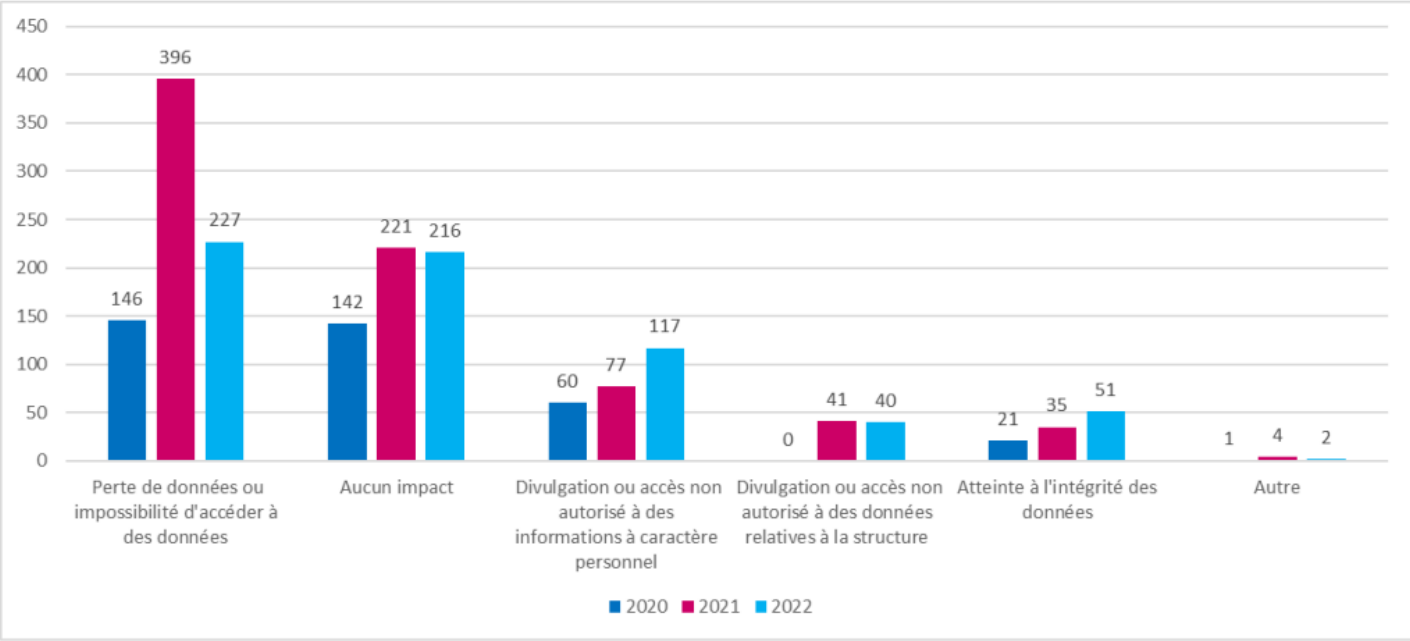


Déclarations selon le type d'impact sur les données

63%
des incidents ont eu un impact sur des données

39%
des structures ont été contraintes de fonctionner en mode dégradé

13%
des incidents ont mené à des mises en danger patient



Notification des vulnérabilités

Une veille quotidienne afin d'alerter les structures dès la publication de la vulnérabilité

Des vulnérabilités permettant d'exécuter du code arbitraire, de réaliser des dénis de service, etc.

15

alertes critiques publiées sur le portail cyberveille-santé

Recommandations et sollicitation du CERT Santé

Durcissement

Réduire la surface d'attaque en **désactivant les comptes, protocoles et services** qui ne sont pas indispensables

Mise à jour

Améliorer le **suivi** et la **correction des vulnérabilités classiques**

Analyse des logs

Analyser **régulièrement les journaux de ses systèmes** et **équipements périmétriques**

Politique de mot de passe

Appliquer une politique de mot de passe suffisamment robuste afin **d'endiguer les actions malveillantes depuis Internet**

Accès renforcés

Renforcer les configurations et la sécurisation des accès en **cloisonnant les réseaux et en effectuant du filtrage**

Gestion des prestataires

Inclure un engagement du prestataire sur le **maintien en conditions de sécurité de son infrastructure**

En cas d'incident il est impératif de **solliciter rapidement le CERT Santé**. Plus tôt l'incident est signalé, plus grande est la probabilité de **contenir et de résoudre la situation de manière rapide** afin de garantir la continuité des services de santé.

semaine européenne DE LA E-SANTÉ

Table ronde : incident de sécurité dans un établissement de santé

Vue métier & opérationnelle

Tour de table

Présentation des intervenants de la table ronde

Jean-Sylvain CHAVANNE
Responsable de la sécurité des systèmes d'information

Oliver CROS
Expert cybersécurité & Réponse à incident

Samuel REJIBA
Directeur des systèmes d'informations

semaine européenne DE LA E-SANTÉ

Détection et confinement de l’incident

Détection et confinement de l'incident

La détection d'un incident cyber nécessite la mise en place de systèmes d'identification d'attaque, mais implique surtout de transmettre les bonnes informations aux bonnes personnes afin de mobiliser le dispositif adéquat pour gérer la gestion de crise et le confinement de l'attaque.

Phase de sidération

- Repérer les signes d'une **activité suspecte** ou d'une atteinte à la sécurité du SI.
- **Signaler et communiquer** rapidement un incident détecté aux personnes et équipes appropriées.
- **Rassembler / coordonner** les différentes équipes compétentes pour gérer l'incident.
- **Déclencher une cellule de crise** si nécessaire.

Confinement

- **Isoler** les ressources critiques.
- **Neutraliser la menace** en limitant la présence malveillante.
- Mise en œuvre de **mesures immédiates** pour empêcher l'attaque de se propager.
- **Protéger le SI, les utilisateurs et les patients.**
- **Mise en œuvre d'un mode dégradé.**

Détection et confinement de l'incident

RISQUES POTENTIELS	BONNES PRATIQUES
Qualification insuffisante et retardée	• **Cartographier** les applications et le SI • Documenter les événements en mettant à jour **le ticket d'incident** • Préparer **les mesures de confinement et les coupures de connexion**
Mauvaise escalade	• **Ne pas attendre et alerter le responsable de crise** en suivant le **processus d'escalade** défini dans la procédure de gestion de crise • Identifier **les réseaux de soutien** (CERT Santé, CERT FR, prestataires, CNIL, etc.) en établissant un annuaire de crise
Mobilisation inefficace	• Mobiliser **les différentes équipes** • Tenir un **annuaire des interlocuteurs de crise** • Réaliser **un kick-off** avec l'ensemble des parties prenantes

« En cas de doute, il n'y a pas de doute »

semaine européenne DE LA E-SANTÉ

Investigation et remédiation technique

Investigation et remédiation technique

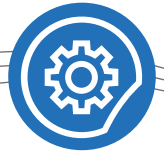
Les investigations doivent être lancées le plus rapidement possible pour améliorer le confinement. Elles sont réalisées tout au long de la crise pour identifier les vecteurs d'intrusion et neutraliser l'attaque

Collecte

Recueillir les **données** et les **informations** pertinentes (journaux, fichiers, etc.) liées à l'incident signalé

Investigation

Evaluation de l'impact de l'incident sur l'ensemble des activités de la structure et identification **des actifs compromis**



Remédiation

Neutralisation de la menace **application des patchs. Redémarrage du SI**

Investigation et remédiation technique

RISQUES POTENTIELS	BONNES PRATIQUES
Investigation lente et peu efficace	• Définir des fiches reflexes **opérationnelles spécifiques** en fonction du type d'attaque • Préparer **en amont les opérations de collecte** • Tracer toutes les informations recueillies dans **la main courante**
Résultat de l'investigation erronée	• Rédiger **une chronologie d'attaque** et tenter de trouver la **date de compromission** • Vérifier **l'origine des preuves reçues** (données en cas de fuite, documents, etc.) • Recueillir **des échantillons, des logs** pour y détecter des **IoCs** et à des fins **d'analyse**
Remédiation peu approfondie	• Prioriser les **services critiques** • Appliquer des **mesures recommandées par les équipes d'investigation** • Reconstruire un **cœur de confiance** • **Ne pas lever le confinement** sans validation formelle

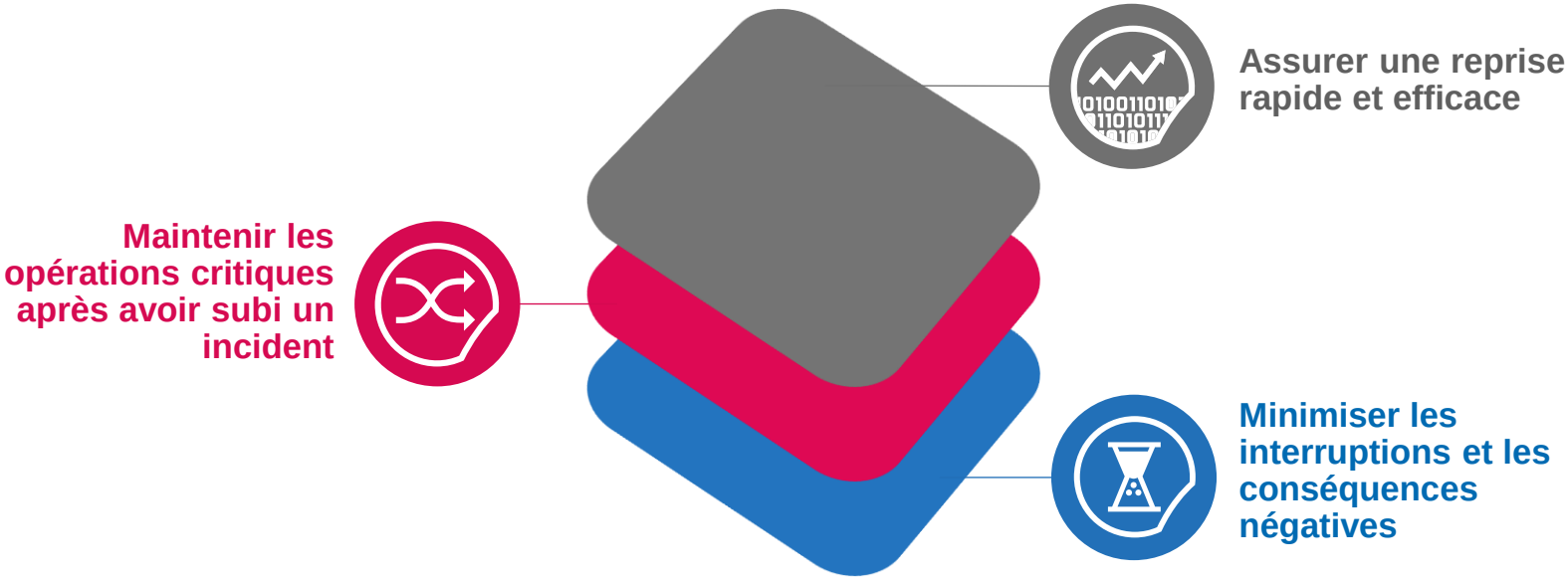
« Mieux comprendre, pour mieux protéger »

semaine européenne DE LA E-SANTÉ

Capacité de maintien en condition opérationnelle

Capacité de maintien en condition opérationnelle (MCO)

Une stratégie de maintien en condition opérationnelle est essentielle pour garantir que les applications, les infrastructures et les matériels puissent continuer à fonctionner et donc limiter les impacts d'une crise cyber



Capacité de maintien en condition opérationnelle (MCO)

RISQUES POTENTIELS	BONNES PRATIQUES
PCA inadapté à l'incident	• **Anticiper les impacts** sur les principaux assets / applications critiques du SI et utiliser une matrice d'impact • Définir la **stratégie de continuité d'activité** et les plans d'action • Définir le **déploiement de solutions de contournement** (solution Cloud, etc.)
PCA mal déployé face à l'urgence	• Appliquer les **mesures de fonctionnement dégradé** en lien avec les plans d'actions • Utiliser du **matériel de secours** (PC, téléphone, serveurs...) • Mettre en place des **mesures palliatives** sur les processus critiques
Remontée incomplète des informations	• Réaliser **un template de synthèse** pour remonter les informations au COMEX et à la cellule de crise • Partager et informer les métiers de tout **changement visible sur le SI** • **Formaliser et vulgariser la synthèse de l'efficacité des plans d'actions** pour transmission aux métiers

« Qui veut la paix prépare la guerre »

semaine européenne DE LA E-SANTÉ

Communication & cohérence des messages

Gestion de la communication

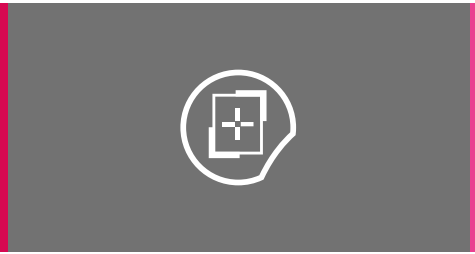
La communication regroupe les dispositifs et actions mis en œuvre par l'établissement afin d'adapter et intégrer à la réflexion l'ensemble des facteurs assurant les prises de décision

Notification initiale

Informer les **équipes internes responsables de la sécurité**

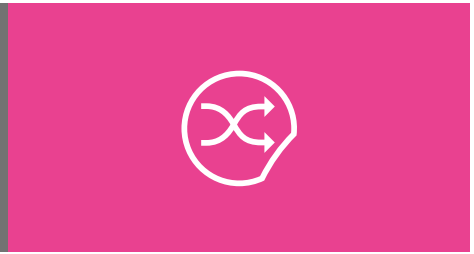
Communication de suivi

Partager les **mises à jour régulières** sur l'évolution de la situation



Communication externe

Communiquer avec **les parties prenantes externes**



Gestion des relations publiques

Préparer des **déclarations publiques,** la gestion **des médias**

Gestion de la communication

RISQUES POTENTIELS	BONNES PRATIQUES
Communication tardive	• **Communiquer de façon régulière** sur la situation de crise auprès des collaborateurs, des partenaires pour assurer une compréhension globale de la situation • S'assurer d'avoir **les bons acteurs** impliqués dès le début de la crise: DPO, RH, CERT Santé…
Panique & perte de réputation	• Avoir une **procédure / kit de communication** interne et externe • **Rendre compte du bruit médiatique** autour de l'événement et nommer des porte-paroles • **Définir une position** vis-à-vis de l'externe, de l'interne, des messages • Ne pas hésiter de s'entourer d'acteurs **dédiées à la communication**
Mauvaise communication interne & externe	• Réaliser des points de situation **courts à intervalles réguliers** • **Utiliser des templates** de main courante et de compte-rendu • **Adapter la description de l'incident à l'ensemble des équipes** • **Fixer les étapes** à suivre et la **réunion suivante** de la cellule de crise

« La communication en temps de crise est un dialogue, pas un monologue »

semaine européenne DE LA E-SANTÉ

Coordination inter-métiers et entre les différentes équipes

Coordination inter-métiers et entre les équipes

Pour faciliter le partage d'information et la capacité d'adaptation, il faut identifier et mobiliser toutes les ressources pour enrayer le développement de la crise et exécuter les actions définies

Coordination inter-métiers et entre les équipes

RISQUES POTENTIELS	BONNES PRATIQUES
Composition de la cellule de crise inadéquate	• Avoir défini la **composition des cellules de crise en amont** y incluant un rôle dédié de coordinateur • Identifier une **salle de crise physique ainsi que virtuelle** • Identifier **des interlocuteurs dédiés** pour échanger avec les parties prenantes (interne et externe)
Mauvaise coordination	• Désigner des coordinateurs de crise permettant **de faire les liens et de faire transiter le bon niveau d'information** entre les équipes • **Ne pas déléguer plus d'actions à un acteur** qui a déjà une action prioritaire en cours
Inaction face à la crise	• Privilégier des **réunions courtes de 15 à 20 minutes** pour favoriser l'action • **Éviter** de traiter des **sujets de moyen ou long terme** • **Désigner un pilote de crise** et lui donner pleinement le rôle de leader • Mettre en place **un rythme régulier de point de situation**

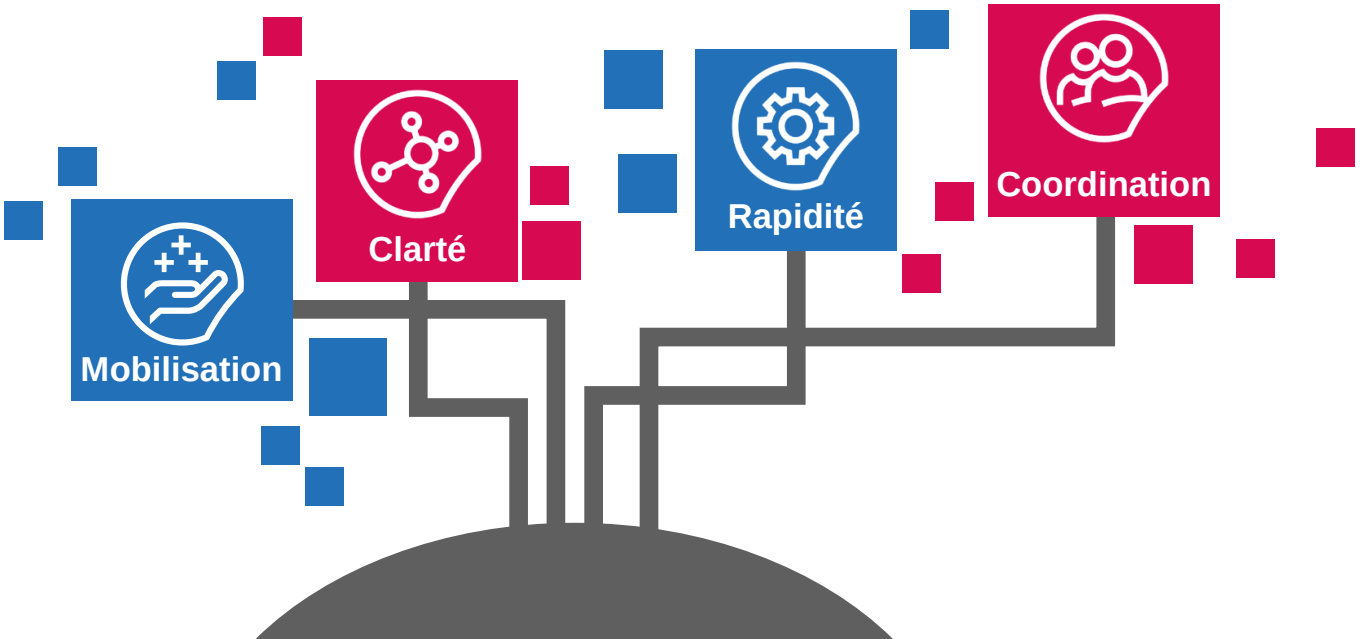
« Communiquer, décider, réagir ! »

semaine européenne DE LA E-SANTÉ

Respect des rôles et des responsabilités

Respect des rôles et des responsabilités

La définition des rôles & responsabilités de chaque partie dans la mise en place d'un dispositif de gestion de crise efficace permet de se mobiliser rapidement dans un mode de crise et de lancer les premières actions opérationnelles et de pilotage



Respect des rôles et des responsabilités

RISQUES POTENTIELS	BONNES PRATIQUES
Absence de dispositif	• Avoir **un dispositif de crise cyber déjà défini** en amont de la crise • Définir **une politique RH de gestion de crise** • Définir **des fiches de rôles** avec les responsabilités clairement explicitées et réparties entre les parties prenantes
Désorganisation humaine	• S'assurer que les bons acteurs soient **mobilisés dès les débuts de la crise** et qu'ils soient au clair avec **leurs rôles et leurs responsabilités** • Avoir **une logistique adaptée gérée par des personnes dédiées** (restauration, logements, moyens de transports, cellule psychologique…)
Indisponibilité & surcharge	• Identifier en amont **des back-ups pour assurer les rotations** • **Rester vigilant sur la charge et la fatigue de chacun**

« Ce n'est pas un sprint, c'est un marathon »

semaine européenne DE LA E-SANTÉ

Annexe

Annexe : questions posées durant la table ronde

Détection et confinement de l'incident

- Quels sont les moyens que vous mettez en place pour **accélérer la prise en charge d'un incident** après sa détection ?
- Quelles **ressources nécessaires** estimez-vous pour définir un **confinement efficace** ?

Capacité de maintien en condition opérationnelle (MCO)

- Comment assurez-vous la **continuité des opérations métier** pendant la résolution d'un incident ?
- Quelles pratiques recommandez-vous pour maintenir **la disponibilité et la performance des systèmes non affectés** par l'incident ?

Coordination inter-métiers et entre les équipes

- Quelles sont les bonnes pratiques mises en place pour faciliter **l'organisation des équipes** et la **prise de décisions** concertées entre les équipes métier impliquées ?
- Quelles sont **les erreurs les plus courantes** liées à la coordination entre les différentes équipes et cellules pendant la gestion d'un incident ?

Investigation et remédiation technique

- Dans le cas d'un incident, quelles sont les priorités de l'investigation ?
- Quelles mesures prenez-vous pour **minimiser l'impact** des investigations techniques sur les activités métier en cours ?
- Quels sont les **services métiers de soins critiques** à redémarrer dans le cadre d'une remédiation ?

Communication & cohérence des messages

- Quelles sont les mesures prises pour garantir que les **messages de communication** sont alignés sur la réalité des faits et évitent toute **spéculation ou désinformation** ?
- D'après vous, quelles contraintes doit satisfaire **un canal de communication** avec les parties prenantes au cours d'un incident ?

Respect des rôles et des responsabilités

- Quelles mesures mettez-vous en œuvre afin d'accompagner les **collaborateurs fragilisés** par une cellule de crise ?
- Quels sont les critères clés que vous utilisez pour **identifier les membres appropriés** qui doivent faire partie de la cellule de crise ?

semaine européenne DE LA E-SANTÉ

Description d’une chaine de compromission

Exfiltration de données & rançongiciel sur l’ESMS
Etape jeunes

e-SANTÉ GRADeS Pays de la Loire

CERT Santé

Tour de table

Présentation des intervenants

Charles BLANC-ROLIN
Chef de projet cybersécurité en santé

Quentin LE THIEC
Expert cybersécurité & Réponse à incident

GRADeS Pays de la Loire & Etape jeunes

l'étape ASSOCIATION
L'INNOVATION AU SERVICE DE L'INSERTION

Localisation : Nantes

Chiffres clés : 230 salariés, 1000 personnes accompagnées, 455 logements.

Secteurs : handicap psychique, protection de l'enfance, grande précarité.

Activités : hébergement et/ou accompagnement

Architecture : hébergement interne des données, 17 serveurs, 3 éditeurs de logiciels

e-santé GRADeS Pays de la Loire

Groupement régional d'appui au développement de la e-santé (GRADeS) : **GCS e-santé Pays de la Loire**

Opérateur préférentiel de l'ARS qui favorise la coopération entre le privé et le public, et entre la ville et l'hôpital. Il propose notamment un **accompagnement autour de la cybersécurité** sous le **pilotage de l'ARS.**

Une offre d'accompagnements diversifiés est proposée aux acteurs de la région autour de la formation, sensibilisation, préparation à la crise, webinaires et appui à la gestion des incidents.

La sécurité numérique en Pays de la Loire

Formations

- Référents sécurité des SI & Animation d'un COPIL sécurité des SI ;
- Séminaire secteur médico-social ;
- Analyse de risques et homologation ;
- Détection et réaction en cas de cyberattaque par rançongiciel

Webinaires

- Sécuriser mon AD ;
- Protéger mes réseaux, mon Wifi ;
- Détecter les menaces ;
- Sécuriser ma messagerie

Journées régionales

- Partager les actualités, nouvelles réglementations et expériences avec les acteurs en région

Base documentaire régionale

- Modèles de documents
- Mémos thématiques
- Base documentaire en ligne

Appui à la gestion des incidents

- Diffusion alertes ;
- Soutien en cas d'incident ;
- Aide à la mise en œuvre d'un outil de supervision réseau

Préparation à la crise cyber

- Soutien à la réalisation d'exercices de crise cyber ;
- Centre de ressource SSI accessibles aux structures les moins dotées (ESMS)
- Synthèse de l'état de l'art de la sauvegarde des données

Veille technologique et réglementaire

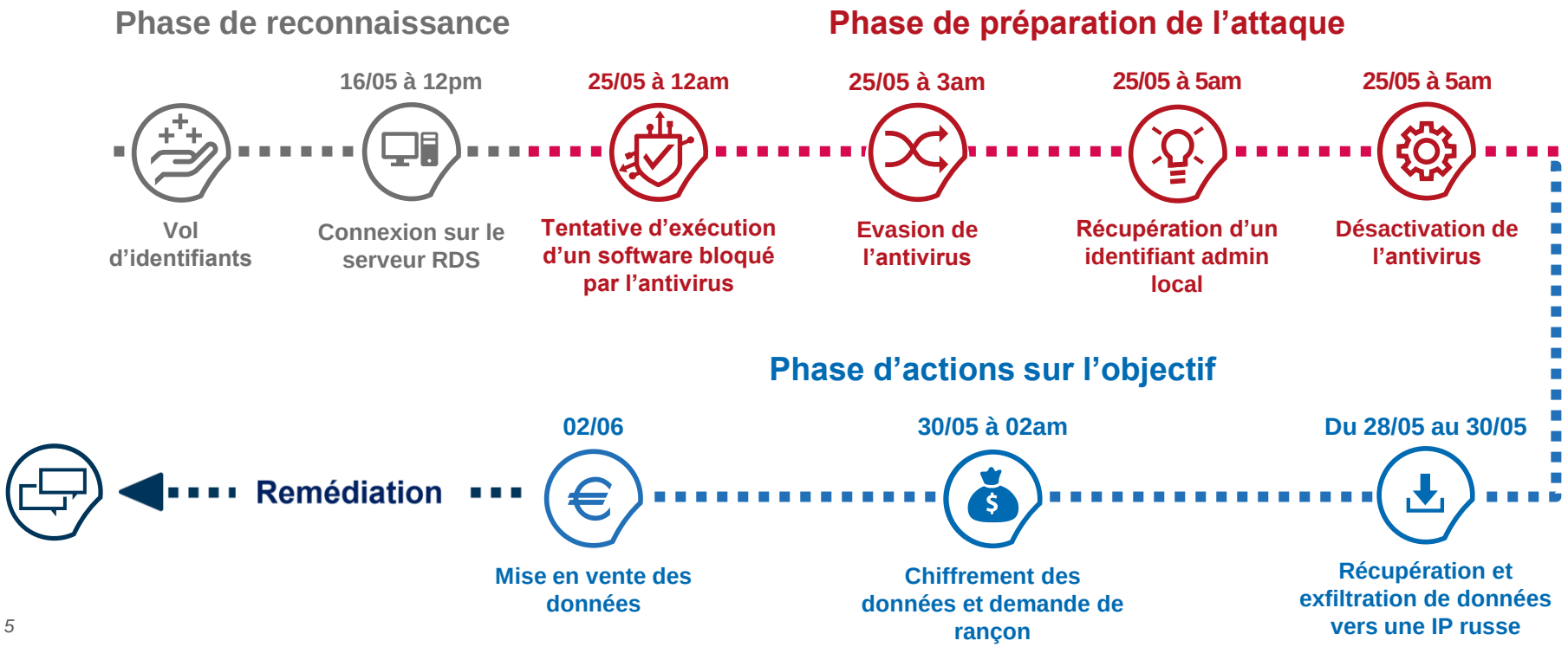
- https://www.scoop.it/t/ssi-sante

Outils de sensibilisation

- Affiches, Fonds d'écran, Escape game, badges métalliques, e-learning, vidéos de sensibilisation, Flyer de sensibilisation des entrepreneurs ,datablockers, faux phishing

Chronologie de l'attaque visant l'Etape Jeunes

Du simple vol d'identifiants à une escalade fulgurante, cette attaque cyber a abouti à des conséquences graves, avec l'exfiltration et le chiffrement de données sensibles.



Etape 1 : Vol d'identifiants

Sensibilisation des utilisateurs

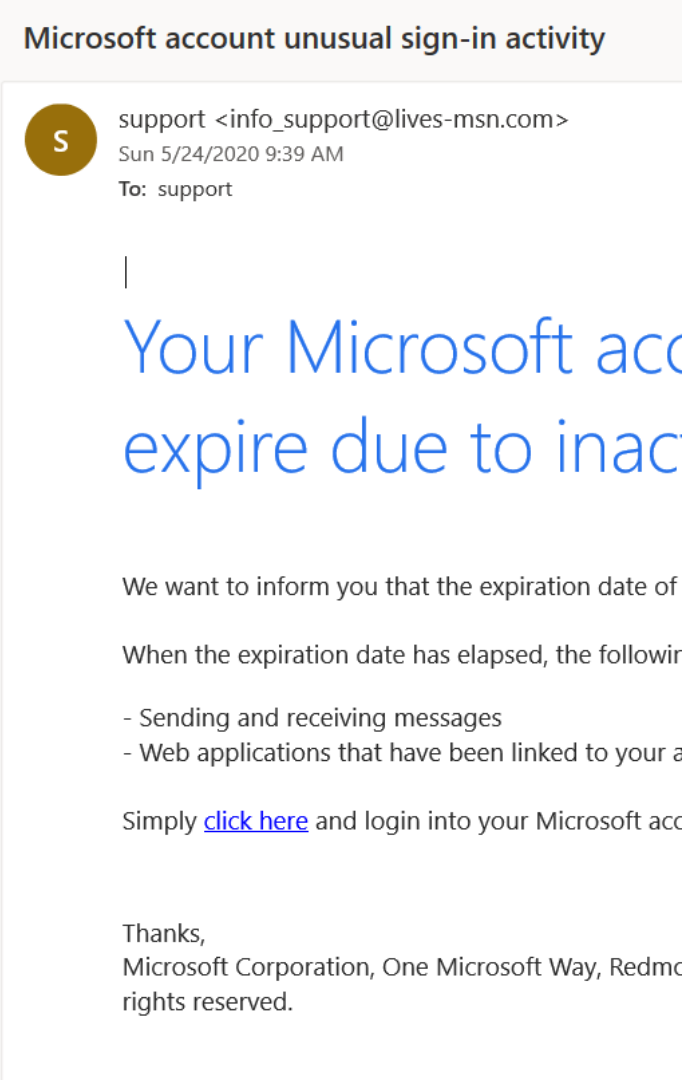
- E-learning & rappel des bonnes pratiques.
- Campagnes de phishing.

Activation MFA

- Mise en œuvre de l'authentification multi-facteur sur l'ensemble des services exposés (Office 365, etc.).
- Implémentation d'un Cloud Access Security Broker (CASB).

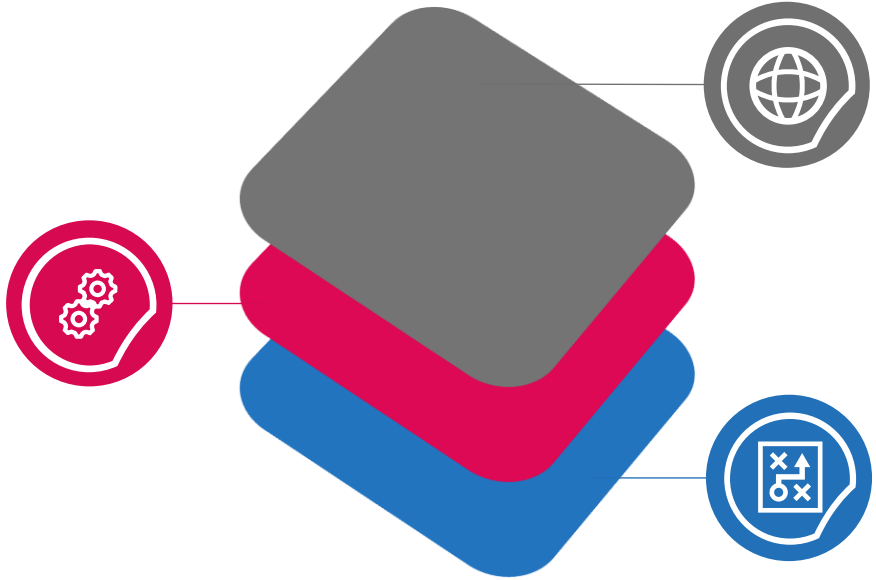
Anti-spam & anti-phishing

- Durcissement protocolaire (DMARC, DKIM, SPF).
- Définition de règles de filtrages.



Etape 2 : Connexion sur le serveur RDS

Après avoir acquis les identifiants volés, l'attaquant peut désormais exploiter la brèche pour se connecter illégalement à un serveur RDS. Cette intrusion lui permet d'accéder à des données sensibles et d'explorer le SI plus en profondeur tout en restant furtif.



Restreindre son exposition directe sur Internet (Implémentation d'un VPN, audit d'exposition, etc.)

Activation de l'authentification multi-facteur

Cloisonner ses réseaux et appliquer un filtrage fin (pare-feu, segmentation, etc.)

Heure	Gravité	Source	Appareil	Description
25 mai 2023, 02:46:46	Attention	Analyse en temps réel		fichier en quarantaine.
il y a 6 jours 25 mai 2023, 02:46:46	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « spyware » dans « mimispool.dll » et a bloqué l'accès au fichier.
il y a 6 jours 25 mai 2023, 02:46:46	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « spyware » dans « mimikatz.dll » et a bloqué l'accès au fichier.
il y a 6 jours 25 mai 2023, 02:46:46	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « spyware » dans « mimidrv.sys » et a bloqué l'accès au fichier.
il y a 6 jours 25 mai 2023, 02:46:46	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « Heuristic.HEUR/AGEN.1321016 » dans « 64.exe » et a mis le fichier en quarantaine.
il y a 6 jours 25 mai 2023, 02:46:46	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « TR/AD.Mimikatz.e81a8f » dans « 86.exe » et a mis le fichier en quarantaine.

Etape 3 : Blocage par l'antivirus

- Activer le blocage automatique des alertes graves
- Surveiller la console de manière régulière
- Durcir la configuration et vérifier l'activité

Etape 5 : Récupération d'identifiant administrateur local

Après avoir été bloqué par l'antivirus, l'attaquant cherche à élever ses privilèges à l'aide d'un outil permettant de récupérer des mots de passe. L'attaquant se reconnecte en RDP au SI en tant qu'administrateur local afin de préparer la phase d'armement et d'exfiltration.

Sécurisation des profils d'admin local

Local Administrator Password Solution (**LAPS**)

Déploiement d'un antivirus

Antivirus couvrant **l'intégralité** du parc informatique

Sécurisation des profils admin de domaine

Admins de domaine dans le groupe *' **protected users** '.*

Supervision des flux réseau

Implémentation **d'outils de supervision** et analyseur de trafic

Etape 6 : Désactivation de l'antivirus

Il s'agit de la conclusion de la phase de préparation : l'attaquant souhaite s'assurer de ne pas pouvoir être détecté et bloqué lorsqu'il commencera à récupérer et exfiltrer les données

Empêcher la désactivation par les administrateurs locaux

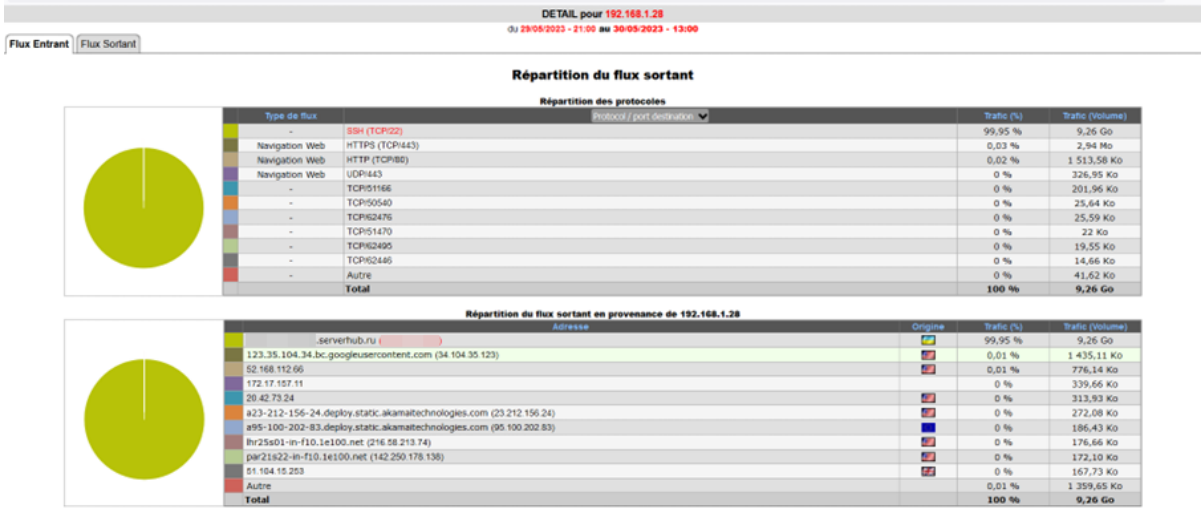
Activer le mode Bloquant au niveau de l'Antivirus

Activer la console centralisée de l'antivirus

Mise en place de règles de détection sur les flux réseaux

Etape 7 : Récupération et exfiltration de données vers une IP russe

L'attaquant réalise une reconnaissance du réseau en vue d'effectuer une latéralisation sur toutes les machines et exfiltrer des informations sensibles (9 Go de données compressées) vers une IP russe.



DETAIL pour 192.168.1.28

du 29/05/2023 - 21:00 au 30/05/2023 - 13:00

Flux Entrant | Flux Sortant

Répartition du flux sortant

Répartition des protocoles

Type de flux	Protocol / port destination	Trafic (%)	Trafic (Volume)
-	SSH (TCP/22)	99,95 %	9,26 Go
Navigation Web	HTTPS (TCP/443)	0,03 %	2,94 Mo
Navigation Web	HTTP (TCP/80)	0,02 %	1 513,58 Ko
Navigation Web	UDP/443	0 %	326,95 Ko
-	TCP/51166	0 %	201,96 Ko
-	TCP/50540	0 %	25,64 Ko
-	TCP/62476	0 %	25,59 Ko
-	TCP/51470	0 %	22 Ko
-	TCP/62495	0 %	19,55 Ko
-	TCP/62446	0 %	14,66 Ko
-	Autre	0 %	41,62 Ko
	Total	**100 %**	**9,26 Go**

Répartition du flux sortant en provenance de 192.168.1.28

Adresse	Origine	Trafic (%)	Trafic (Volume)
.servertuh.ru ( )		99,95 %	9,26 Go
123.35.104.34.bc.googleusercontent.com (34.104.35.123)		0,01 %	1 435,11 Ko
52.168.112.66		0,01 %	776,14 Ko
172.17.157.11		0 %	339,66 Ko
20.42.73.24		0 %	313,93 Ko
a23-212-156-24.deploy.static.akamaitechnologies.com (23.212.156.24)		0 %	272,08 Ko
a95-100-202-83.deploy.static.akamaitechnologies.com (95.100.202.83)		0 %	186,43 Ko
lhr25s01-in-f10.1e100.net (216.58.213.74)		0 %	176,66 Ko
par21s22-in-f10.1e100.net (142.250.178.138)		0 %	172,10 Ko
51.104.15.253		0 %	167,73 Ko
Autre		0,01 %	1 359,65 Ko
Total		**100 %**	**9,26 Go**

Gestion des protocoles & flux

- Définition d'alertes sur les flux.
- Filtrer & limiter les protocoles.

Diffusion de données sur Internet

- Restriction des données pouvant sortir de la structure.
- Surveiller les mises en vente de données sur internet.

Etape 8 : Chiffrement des données et demande de rançon

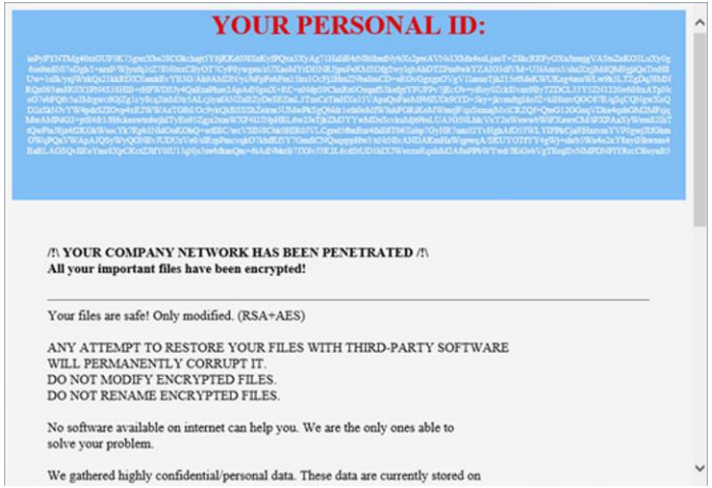
Après avoir exfiltré des informations, l'attaquant exécute le malware de chiffrement (attack12.exe) sur l'ensemble du SI et décide de mettre en vente les données sur le dark web.

Signaler l'incident & Demander de l'aide

Déconnecter du réseau les machines (ne pas les éteindre ni les allumer)

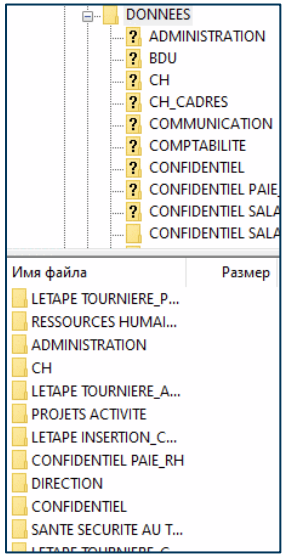
Investigation et remédiation

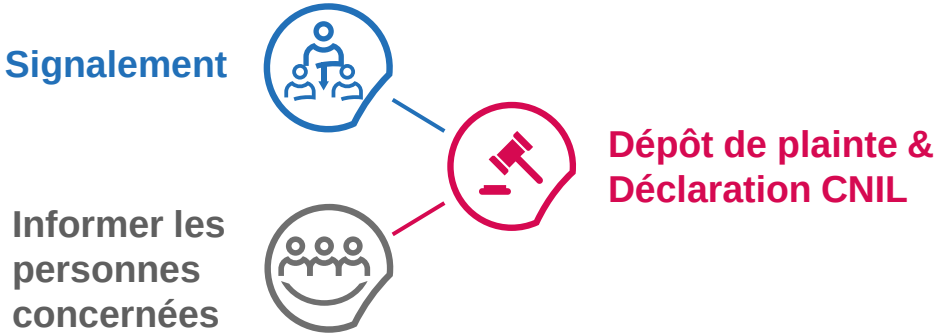
Disposer de sauvegardes intègres



Etape 9 : Mise en vente des données

Le site de rançongiciel annonce avoir en sa possession des données sensibles appartenant à l'Etape Jeunes et propose de les revendre. Parmi ces données, de nombreuses données confidentielles sont disponibles.





Remédiation & durcissement

Revues régulières

- Processus
- Configurations sécurisées
- Documentations

Durcissement des sauvegardes

- Authentification locale et robuste (MFA)
- Déconnectée du réseau et hors site (à froid)

Exigences contractuelles

- Définition des rôles et contractualisation des responsabilités
- Engagements de sécurité

semaine européenne DE LA E-SANTÉ

Une réponse collective, le Programme Cybersécurité accélération et Résilience des Etablissements (CaRE)

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

DIRECTION GÉNÉRALE DE L'OFFRE DE SOINS

ars Agence Régionale de Santé

GRADeS

Délégation ministérielle au numérique en santé

AGENCE DU NUMÉRIQUE EN SANTÉ

Tour de table

Présentation des intervenants

Auriane LEMESLE
Référente régionale Sécurité des Systèmes d'Information

Elodie CHAUDRON
Directrice de programme

Fabian RICHARD
Responsable e-santé & transformation numérique

Jean-Baptiste LAPEYRIE
Directeur expertise, innovation et international

Silvère RUELLAN
Chef du bureau cybersécurité santé et affaires sociales

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté Égalité Fraternité

Genèse et ambitions du programme CaRE

Délégation ministérielle au numérique en santé

AGENCE DU NUMÉRIQUE EN SANTÉ

Lancement de la TF cyber suite à la cyberattaque du CHSF

Des ambitions :

- Concevoir un **plan massif pluriannuel** sur 2023-2027
- Une volonté **d'engager une grande majorité des ES** sur 2023-2024
- Obtenir des **résultats concrets** dès maintenant pour la résilience des ES
- **Accompagner l'ensemble des ES** dans leur montée en maturité sur la cybersécurité

Des financements :

- « **Ponctuel** » pour permettre de franchir un cap
- « **Annuel** » pour maintenir le niveau acquis et considéré comme le « Socle Cyber »
- « **Offre de services** » pour développer et coordonner l'offre de services nationale et régionale, pour un déploiement massif au sein des ES

Programme CaRE

« Une réponse collective, déterminée et coordonnée pour faire face à la menace »

Une TF regroupant toutes les parties prenantes

Une équipe cœur

- DNS
- FSSI
- DGOS
- ANSSI
- ANS
- ARS
- GRADeS

Et des contributeurs

- Fédérations Hospitalières
- Fédérations Médico-sociales
- Etablissements de santé
- Industriels
- Centrales d'achat

Une feuille de route déclinée en 4 axes

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

Une feuille de route articulée autour de 4 axes

AXE 1 - Gouvernance et Résilience

Objectifs

- Intégrer la cybersécurité dans la **gouvernance** des établissements
- Intégrer un **volet numérique dans le plan blanc** des établissements, puis formaliser et mettre en œuvre un **plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA),**
- Réaliser annuellement un **exercice de gestion de crise cybersécurité** pour les ES et engager la dynamique pour les ESSMS,
- Engager les ES et les ESSMS dans une **démarche d'auto-évaluation** de leur niveau de maturité cyber et d'orientation de leur feuille de route cybersécurité.

Travaux en cours

- **Exercices de crise ES** : + 500 exercices réalisés
- **Kit exercice régional** (ARS + préfecture)
- **Kit PCA / PRA** : démarrage phase pilote
- **Trame CPOM ARS ES** : test à venir dans un GHT
- **Certification HAS 2024** : intégration de critères numériques

Une feuille de route articulée autour de 4 axes

AXE 2 - Ressources et mutualisation

Objectifs

- Favoriser la **mutualisation des ressources et des moyens** entre établissements
- Augmenter le **nombre de personnels dédiés à la SSI** notamment opérationnelle dans les établissements
- Garantir dans chaque établissement un **budget numérique suffisant** dédié exclusivement à la cybersécurité
- Développer une **offre de service répondant aux besoins** prioritaires des établissements, en lien avec les GRADeS et les acteurs industriels

Travaux en cours

- Renforcement **grilles RH** (DGOS)
- Recensement **offre de services** via constitution d'un catalogue (publication fin septembre)
- Définition en cours du con**tenu des centres de ressources cyber des GRADeS**
- Travaux en cours avec **les industriels en lien avec les besoins du programme**

Une feuille de route articulée autour de 4 axes

AXE 3 - Sensibilisation

Objectifs

- Sensibiliser prioritairement **les directions d'établissements** sur le risque cybersécurité et ses impacts
- Animer une **communauté des RSSI d'établissement**
- Sensibiliser plus largement **l'ensemble du personnel** des établissements
- Intégrer l'hygiène informatique dans la **formation initiale et continue** des professionnels

Travaux en cours

- **Campagne de communication ciblée** sur les publics prioritaires en cours (Tous cybervigilants V2)
- Réalisation de pastilles vidéos **RETEX d'ES cyberattaqués**
- **Formation sur la cybersécurité** en accès libre sur la plateforme e-santé formation
- **Evènements nationaux et régionaux**

Une feuille de route articulée autour de 4 axes

AXE 4 - Sécurité opérationnelle

Objectifs

- **Rattraper le retard** puis **maintenir le niveau acquis** via l'atteinte d'objectifs considérés comme le « Socle Cyber » et faciliter l'engagement de dépenses pluriannuelles
- Disposer d'une capacité d'audit / contrôle des ES permettant **d'attester l'atteinte des objectifs** des différents financements et de valider le niveau d'avancement du programme CaRE
- **Renforcer la sécurité des ES et ESSMS** : exposition sur internet, annuaires d'établissement, postes de travail, accès au SI depuis l'extérieur, sauvegardes

Travaux en cours

- Publication **premier appel à financement** fin octobre 2023 : sécurisation exposition internet et maitrise annuaire d'établissements (60 M€)
- Objectif : publication régulière d'appels à financement sur des **sujets identifiés comme prioritaires**

Les Jeux Olympiques 2024

- **Mise en place d'un groupe de travail dédié piloté par le FSSI, et regroupant la DNS, la DGOS, l'ANSSI, l'ANS et les 7 ARS concernées par les JOP**
- **Identification de 220 ES critiques**
- **Suivi mensuel de ces ES sur l'atteinte d'un certain nombre d'objectifs :**
  - Alimentation d'OPSSIES sur les mesures prioritaires en SSI
  - Réalisation d'exercices de crise (un en 2023, un en 2024)
  - Contractualisation avec un prestataire de réponse à incidents à l'échelle de la région ou du GHT
  - Réalisation d'audits : ADS et SILENE (ANSSI), cybersurveillance (CERT Santé), audits de passerelles de messagerie (CERT Santé)
- **Quelques précisions complémentaires :**
  - Mise à disposition du kit **régional d'exercice de crise** mi-septembre 2023
  - **Phase pilote PCA / PRA** : 15 ES prioritaires dans la liste des pilotes retenus
  - **Tous les ES (publics et privés)** peuvent demander la réalisation d'audits par l'ANSSI
  - Identification des **autres leviers possibles** en cours (ANSSI)

PARIS 2024 PARIS 2024

FSSI
Patrice BIGEARD
patrice.bigeard@sg.social.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

POINT D'ACTUALITÉ SUR NIS 2

Une directive destinée à assurer un niveau élevé commun de cybersécurité dans toute l'UE

NIS pour Network and information system security

Directive NIS 1 publiée en 2016 et transposée au niveau national en 2018

- ~300 opérateurs concernés tous secteurs confondus, 142 dans la santé, dont 135 en tant qu'établissement support de GHT

Directive NIS 2 publiée en décembre 2022, en cours de transposition, d'ici octobre 2024

Principaux changements avec NIS 2 :

- Extension du champ d'application, avec plusieurs milliers d'entités concernées, > 1 000 rien que dans la santé
- Mécanisme de proportionnalité avec deux catégories d'entités, essentielles (EE) ou importantes (EI), selon leur taille et criticité
- Renforcement du régime de sanction, avec un mécanisme comparable à celui du RGPD

Les entités concernées dans le secteur santé

(présentation simplifiée, les travaux de définition précise du périmètre sont en cours)

Type d'entité (au sens de la directive)	> 250 employés	50 à 250 employés	< 50 employés
Prestataires de soins de santé	**Entités essentielles (EE)**	**Entités importantes (EI)**	**Hors périmètre NIS2**
Laboratoires de référence de l'UE			
Entités fabriquant des produits pharmaceutiques			
Entités de R&D dans le domaine des médicaments			
Entités fabriquant des dispositifs médicaux (DM) [1]			
Organismes de recherche [2]			

[1] Ces entités relèvent des EI, à l'exception des entités fabriquant des DM critiques en cas d'urgence de santé publique, qui relèvent des EE.
[2] Organismes de recherche non limités au secteur santé.

Les obligations pour les entités régulées

Principes généraux, en cours de définition précise :

- **Se notifier à l'ANSSI et lui communiquer des informations de contact à jour** (pas de désignation unitaire par arrêté comme c'était le cas avec NIS 1)

- **Déclarer à l'ANSSI les incidents majeurs** (déclaration initiale, rapport d'avancement, rapport final)

- **Mettre en œuvre les mesures prévues en matière de gestion des risques cyber** : mesures relatives à l'analyse des risques, la gestion des incidents, la continuité des activités, l'authentification, l'acquisition/développement/maintenance des SI, etc.)

Prochaines étapes

Deux démarches en cours pour :

- Transposer la directive en droit national d'ici octobre 2024 (projet de loi en préparation)
- Préparer la mise en œuvre opérationnelle, avec transformation de l'action de l'ANSSI pour passer à l'échelle : développement de services numériques, adaptation de l'accompagnement, appui sur des relais, etc.

Pour alimenter ces travaux : consultation des ministères et des acteurs des différents secteurs sur le S2 2023

- Consultation des acteurs sur 3 thèmes :
  - Le périmètre des entités régulées (qui est concerné ? en tant qu'EE ou EI ?) ➔ consultation en cours (du 13/09 au 20/10)
  - Les interactions entre les entités régulées et l'ANSSI (que dois-je communiquer à l'ANSSI et comment ?) ➔ webinaire de lancement le 10/10
  - Les mesures de sécurité (que dois-je mettre en œuvre ? comment m'y prendre ?) ➔ webinaire prévu en novembre 2023
- Consultation via les organisations professionnelles de chaque secteur
  - Organisations contactées pour la santé : FHF, FHP, FEHAP, Unicancer, FNEHAD, SYNERPA, LEEM, France Biotech, SNITEM, SIDIV
  - Délai de 6 semaines à compter de chaque webinaire pour que les organisations consultées transmettent leurs retours à l'ANSSI

Pour aller plus loin

La directive NIS 2 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555

La page dédiée sur le site de l'ANSSI avec une FAQ enrichie au fil de l'eau :
https://www.ssi.gouv.fr/directive-nis-2

Points de contact à l'ANSSI :

- Silvère RUELLAN, chef du bureau santé et affaires sociales, **Silvere.RUELLAN@ssi.gouv.fr**
- Laure DUHESME, coordinatrice sectorielle santé, **Laure.DUHESME@ssi.gouv.fr**