Lundi de la Cybersécurité

MANIKA

Au secours, je suis victime d'un hacker !

Lundi 13 mars 2023

Lionel MOURER

Directeur Général de MANIKA / Consultant Principal

Administrateur du CLUSIF

L'intervenant : Lionel MOURER

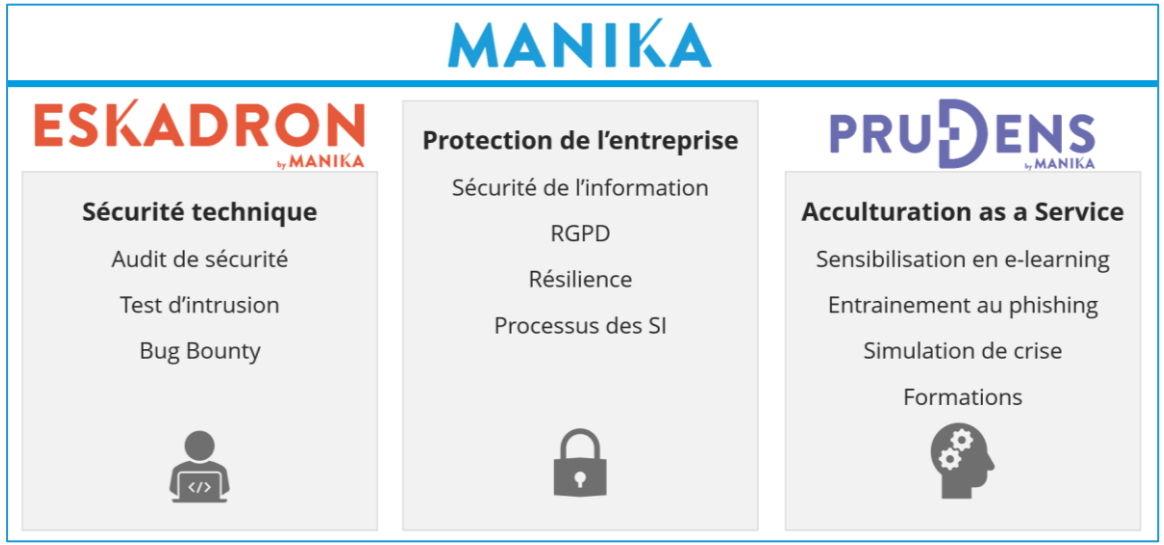
- Expérience
  - +35 ans d'expérience dont +23 dans la SSI / CA
  - Directeur Général de MANIKA (ex-ATEXIO) et Consultant Principal
- Domaines et compétences
  - sécurité de l'information & résilience (continuité d'activité / gestion de crise)
  - conseil méthodologique
    - ISO 27001, ISO 22301 et PSSI, PCA/PUPA, Gestion de crise
  - formation et sensibilisation (intra & inter)
  - audits organisationnels
    - analyse des risques (ISO 27005, EBIOS)
- Divers
  - administrateur du CLUSIF
  - membre du CCA (ex-administrateur)
  - membre de l'AFNOR (commissions « Sécurité des Systèmes d'Information » et « Sécurité & Résilience »)
  - formateur écoles (Télécom SudParis, CESI, IMT-BS, IMT Lille, etc.)
  - formateur instituts (CyberAcademy, HS2, Afnor Compétences, PLB, etc.)
- Formation
  - ingénieur en Technologie de l'Information
  - IMT Lille (ex-Télécom Lille / ENIC – promo. 1999)

Fiche d'identité du Cabinet

- Données clés
  - création en 2013
  - SAS au capital de 40 000 €
  - Filiale du groupe NEXTEDIA (CA : +50 M€, +350p)
- 30 personnes
  - + 10 ans d'expérience en moyenne
- Corpus documentaires / Offres
  - SMSI, ISDP, RGPD
  - SMCA, PCA, PCIT, GDC
  - rapports OWASP / ANSSI
- Impliqué dans les groupes de travail « références »

CLUSIF CCA Club de la Continuité d'Activité afnor CLUBEBIOS AFCDP Association Française des Correspondants à la protection des Données à caractère Personnel

- Nos offres
  - Conseil, audit, formation



- Labels et certifications

GOLD 2022 ecovadis Sustainability Rating

THE GLOBAL COMPACT
NOUS SOUTENONS LE PACTE MONDIAL

LABEL FOURNISSEUR provigis CONFORME 2020

Sommaire

- Qu’est ce qui peut provoquer une cyber-crise ?
- Conséquences d’une cyber-crise
- Deux réactions possibles
- Gestion d’une cyber-crise…

Sommaire

- Qu’est ce qui peut provoquer une cyber-crise ?
- Conséquences d’une cyber-crise
- Deux réactions possibles
- Gestion d’une cyber-crise…

Facteurs Humains (*malware* & piratage) (1/2)

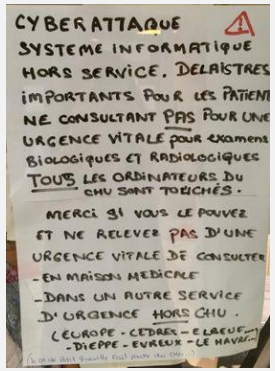
Juin 2016

- 4 jours de gestion de crise, 10 pour que l'activité reprenne totalement
- « NotPetya nous a coûté 220 M€ de chiffre d'affaires et 80 M€ de résultats » (Claude IMAUVEN, DG exécutif de Saint Gobain)

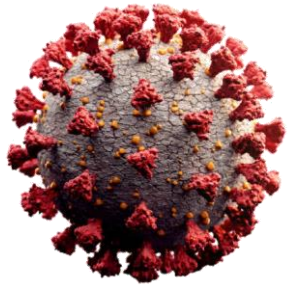
Stuxnet 2010
Locky 2016
WannaCry 2017
NotPetya 2017

Novembre 2019

- Vers 19H… : attaque informatique de grande ampleur, impactant fortement le SI et l'activité
- Chiffrement de certains fichiers situés sur des ordinateurs et des serveurs
- Retour à la normale après plusieurs jours
- Plainte contre X déposée



COVID-19 = TRÊVE ?…



LCI

Les hackers promettent de ne pas s'attaquer aux hôpitaux durant l'épidémie de coronavirus

iStock

TRÊVE – Quelques-uns des groupes de hackers les plus actifs pour tenter des opérations de ransomware (rançonnage) ont annoncé qu'ils ne s'attaqueront pas aux établissements de santé durant la pandémie de coronavirus.

19 mars 2020 10:33 - Melinda DAVAN-SOULAS

Centre Hospitalier Dax-Côte d'Argent

9 fév. 2021

l'hôpital NORD OUEST Villefranche-sur-Saône Tarare

15 fév. 2021

CENTRE HOSPITALIER ALBERTVILLE MOUTIERS

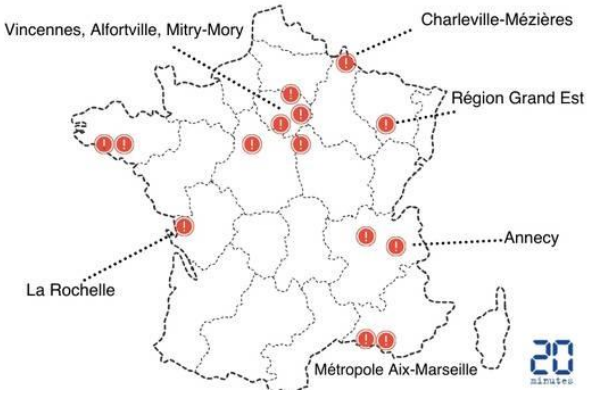
21 déc. 2020

Covid-19 : les cyberpirates qui ont attaqué l'Agence européenne des médicaments ont manipulé des documents sur les vaccins franceinfo avec AFP 15 janv. 2021

Allemagne. Une cyberattaque contre une clinique provoque la mort d'une patiente 11 et 12 sept. 2020

Cybersécurité des hôpitaux : «27 attaques majeures en 2020 et une par semaine en 2021» Le Figaro avec AFP 17 fév. 2021

Principales collectivités victimes d'un rançongiciel en 2020



Facteurs Humains (*malware* & piratage) (2/2)

Avril 2020

- À la suite d'une mise à jour, les données des créateurs de cagnotte Leetchi étaient accessibles depuis la page de la cagnotte

Une erreur technique a échappé à notre vigilance et entraîné une perte de confidentialité de vos données personnelles *(nom, prénom, date de naissance, e-mail et coordonnées GPS)*. Ces données ont été rendues visibles dans le code source de la page de votre cagnotte et nous tenions à vous en informer.

Soyez rassuré·e **les fonds collectés** et **vos informations bancaires** sont toujours restés **inaccessibles et en sécurité sur notre plateforme**.

Octobre 2021

- Iran : cyberattaque entraîne une panne générale de distribution de carburant
- 24 heures après, seules 220 stations-service (sur 4 300) ont pu être reconnectées au système central de distribution

Facteurs Humains (*malware* & piratage) (2/2)

Décembre 2022

LastPass •••

- Phase 1 : l'ordinateur portable d'un ingénieur logiciel a été compromis ➔ accès à un environnement de développement basé sur le cloud et vol de code source, d'informations techniques et certains secrets du système interne de LastPass
- Phase 2 : un ingénieur DevOps senior ciblé, via l'exploitation d'un logiciel tiers vulnérable ➔ diffusion de logiciels malveillants, contournement des contrôles existants et obtention d'un accès non autorisé aux sauvegardes dans le cloud
- Les données consultées comprenaient des données de configuration du système, des secrets d'API, des secrets d'intégration de tiers et des données chiffrées et non chiffrées sur les clients de LastPass.

Mars 2023

- Après Hensoldt France et Hemeria…
- Ingenico
- Groupe cybercriminel Snatch

Sommaire

- Qu’est ce qui peut provoquer une cyber-crise ?
- Conséquences d’une cyber-crise
- Deux réactions possibles
- Gestion d’une cyber-crise…

Les conséquences / impacts d'une crise

- Business Activité

- Juridique

- Financiers

- Image de marque

- Humains / Sociaux / autres

Sommaire

- Qu’est ce qui peut provoquer une cyber-crise ?
- Conséquences d’une cyber-crise
- Deux réactions possibles
- Gestion d’une cyber-crise…

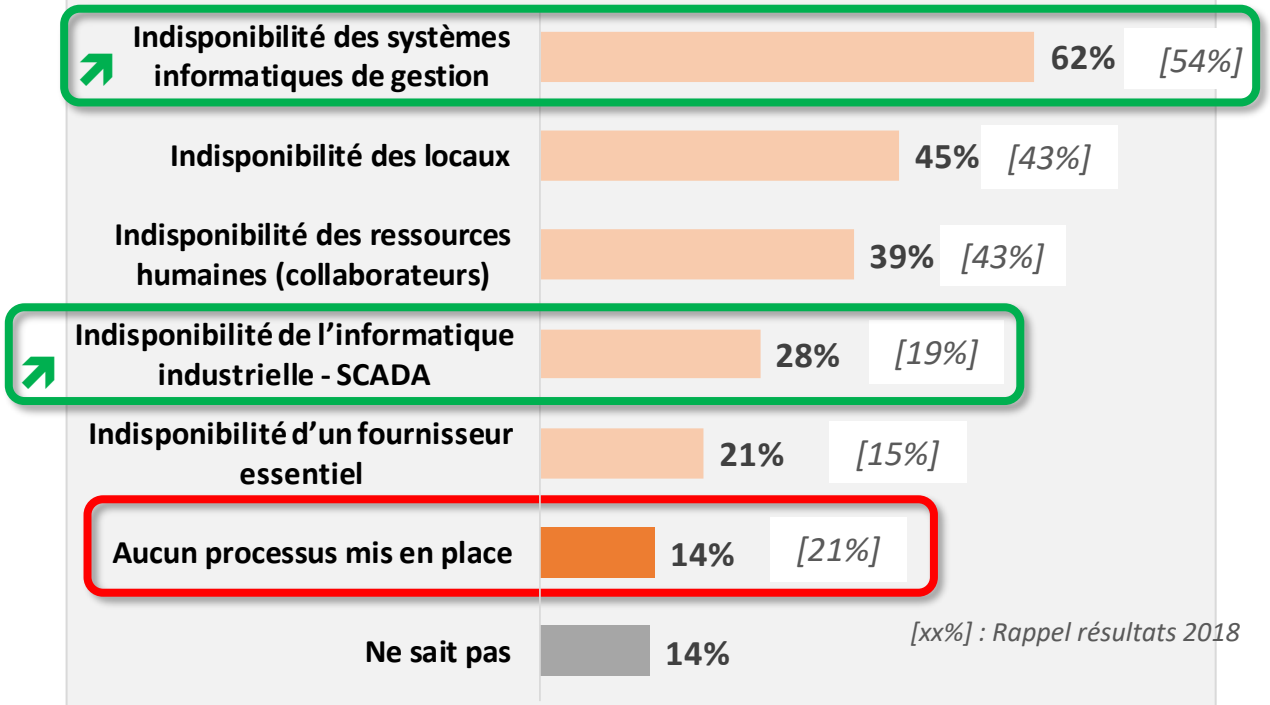
Alors, comment on gère ???...

On adresse le problème...	...ou pas !!!

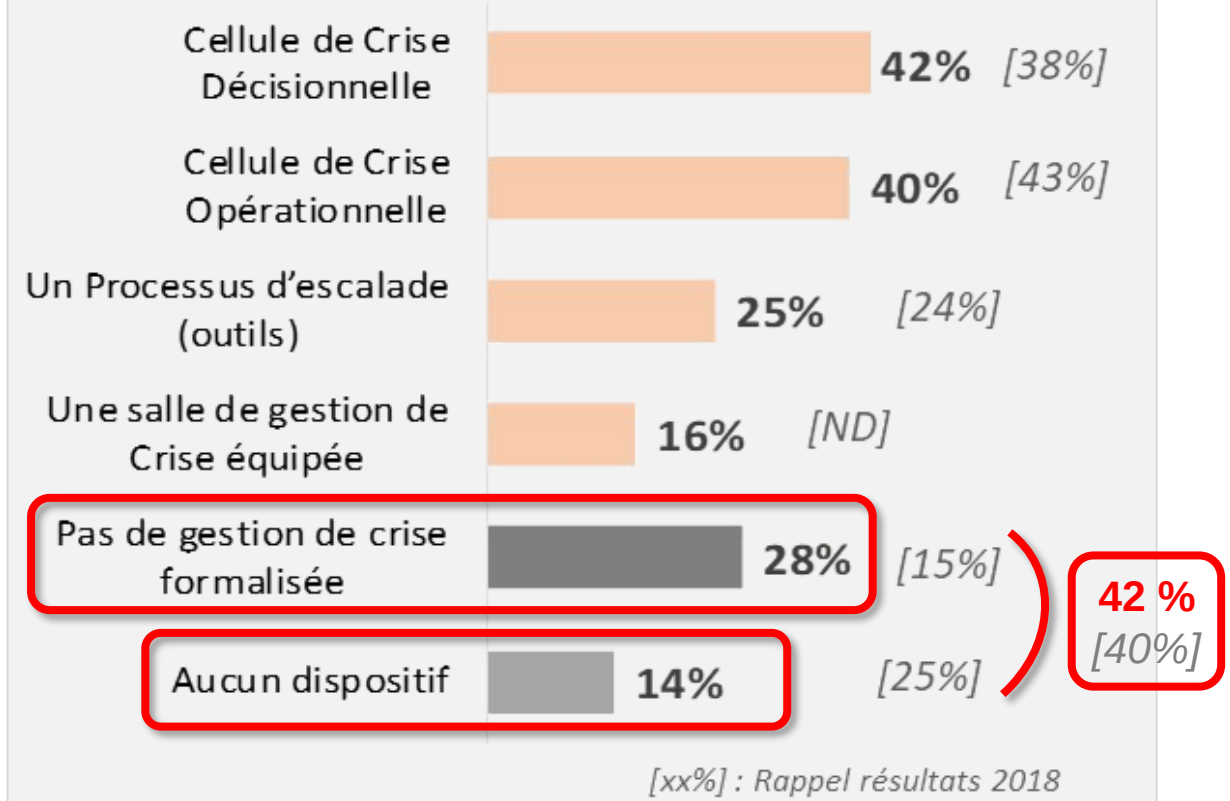
Étude MIPS 2020 - Entreprises vs Continuité d'Activité et Gestion de crise

https://clusif.fr/publications/mips-2020-menaces-informatiques-et-pratiques-de-securite-en-france-edition-2020-rapport-global/

La gestion de la continuité d'activité dans votre entreprise couvre-t-elle les scénarii suivants* ?



La gestion de crise dans votre entreprise comprend-elle*?



* Plusieurs réponses possibles

Mise en œuvre du PCA – Domaines traités

3 + 1 domaines distincts sont abordés dans un Plan de Continuité d'Activité

Gestion de crise

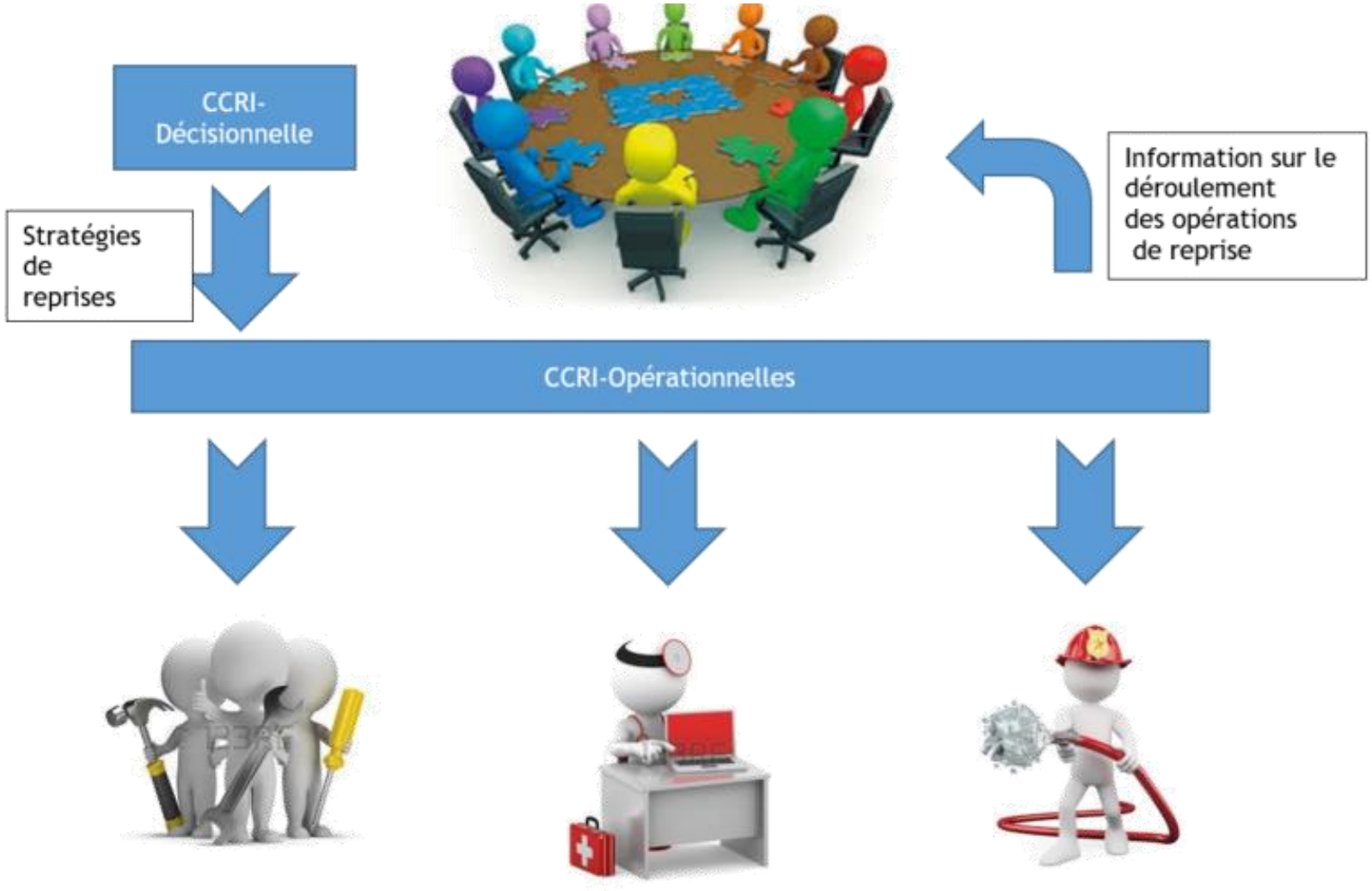
Communication	Reprise des activités 'métier'	Continuité IT

Sommaire

- Qu’est ce qui peut provoquer une crise ?
- Conséquences d’une crise
- Deux réactions possibles
- Gestion d’une cyber-crise…

Gestion de crise…

- Cellule de crise
  - définit la stratégie
    - en fonction du sinistre
  - valide les plans spécifiques à activer
  - arbitre en temps réel
  - valide la stratégie de retour à la normale



Gestion de cyber-crise…

- Spécificités d'une attaque cyber
  - moins visible (en première intention…) que les autres types d'attaques / sinistres
  - difficile d'évaluer
    - durée de l'attaque : depuis combien de temps ?…
    - étendue de l'attaque : quel périmètre ?…
    - réalité de l'attaque : chiffrement, vol des données, rebond, black-out ?…
  - besoin substantiel de compétences « informatiques »
    - interne : rareté
    - externe : qui peut / doit m'aider ?…
  - « mon SI est attaqué »
    - diminution de la capacité de réponse !!!
    - les processus de continuité d'activité « classiques » répondent-ils au besoin ???

Gestion de cyber-crise…

- Se préparer

  (la crise arrive, n'en doutez pas…)

  - identifier le patrimoine informationnel
    - typologie des données
      - personnelles, R&D, bancaires, etc.
    - sensibilité
      - critères DIC T P A…
    - attractivité
      - intérêt et/ou valeur (pour qui et pour quoi faire ?)
    - localisation
      - comment et où sont-elles stockées / sauvegardées ?
    - circulation
      - comment se les échange-t-on, qui les administre, etc.

  - mettre en place des mesures de prévention / protection pour limiter le risque d'attaque
    - sauvegarder les données (pas – seulement – online !!!)
    - maintenir à jour les systèmes et les applications
    - cloisonner le système d'information
    - limiter au strict nécessaire les droits des utilisateurs et les autorisations des applications
    - maîtriser les accès Internet
    - sensibiliser les collaborateurs
    - contracter une assurance cyber
    - mettre en œuvre un plan de réponse aux cyberattaques
    - penser sa stratégie de communication de cyber-crise
    - auditer régulièrement le système d'information

Gestion de cyber-crise …

- Détecter

  (tiens, serait-ce une crise, par hasard ?…)

  - en temps réel 😃
    - IPS/IDS
    - SOC / SIEM – 24/7

  - en temps différé 😖
    - analyse a posteriori des journaux (logs)
    - contact par les attaquants…
    - publication dans la presse…

Gestion de cyber-crise …

- Réagir (1/2)

  (la crise est là : on fait quoi ??!!…)

  - identifier le « scénario » d'attaque
    - temps T0 et chemin d'attaque
  - dérouler les protocoles préétablis
  - prendre des mesures conservatoires
    - confiner
      - mettre en quarantaine les postes informatiques concernés par l'incident
    - isoler
      - couper tous les accès réseaux pour stopper l'incident
    - sauvegarder
      - les journaux d'activités (connexions Web, événements systèmes, etc.
      - le trafic réseau supervisé (firewalls, IDS, etc.)
    - collecter les renseignements internes
      - auprès des premières personnes à avoir détecté l'incident et à avoir donné l'alerte
      - auprès des personnes témoins de l'incident
    - collecter les renseignements externes
      - auprès des prestataires de services (télécommunications, développement d'application, maintenance des matériels, etc.)
    - communiquer
      - aux personnels ciblés de l'entreprise les recommandations adaptées à la gestion de l'incident

Gestion de cyber-crise …

- Réagir (2/2)

  (la crise est là : on fait quoi ??!!…)

  - prévenir les « autorités »
    - https://clusif.fr/cyber-victimes/
    - https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Le-ministere-de-l-interieur-mobilise-face-aux-cybermenaces
    - https://www.ssi.gouv.fr/en-cas-dincident/
    - https://www.cybermalveillance.gouv.fr/diagnostic/accueil
  - aller chercher de l'aide
    - assureurs (si vous avez souscrit…)
    - experts internes (si vous en avez…)
    - experts externes / prestataires de réponse aux incidents de sécurité qualifiés (PRIS) (s'ils sont disponibles…)
  - rançon : « *To pay or not to pay…* »
  - porter plainte

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Centre de lutte contre les criminalites numeriques

CELLULE FRANCAISE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

Gestion de cyber-crise …

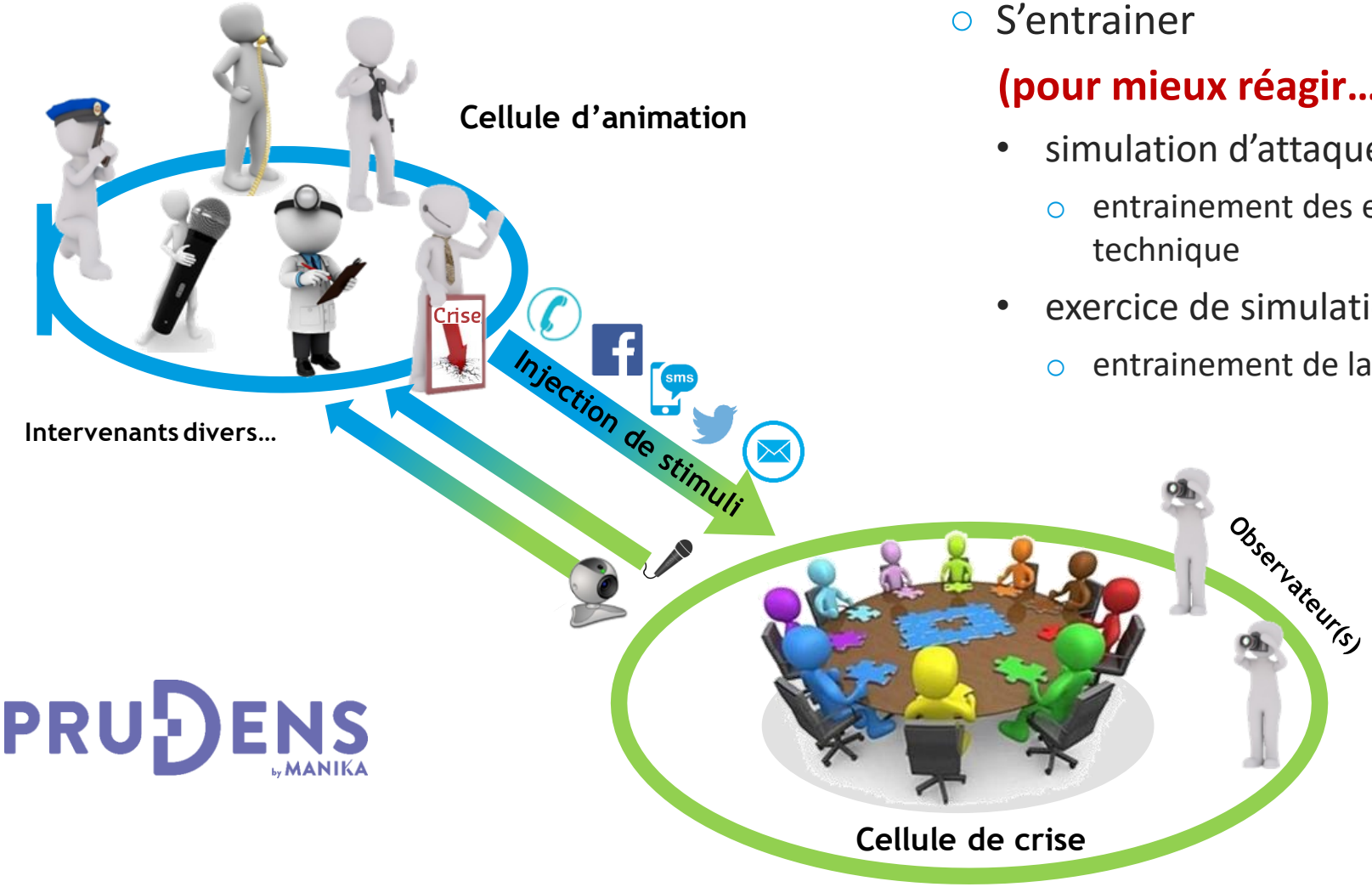
- Rétablir

  (la crise est passée : je reviens à la normale…)

  - corriger la vulnérabilité initialement utilisée par l'attaquant
  - vérifier l'absence de modifications réalisées par le programme malveillant lui permettant de se maintenir après le redémarrage d'une machine précédemment infectée
  - restaurer les systèmes, applications, données depuis des sources saines
  - changer les mots de passe

  - un peu plus tard, mais pas trop tard…
    - formaliser un retour d'expérience !

Gestion de cyber-crise …



PRUDENS by MANIKA

- S'entrainer

  (pour mieux réagir…)

  - simulation d'attaque cyber
    - entrainement des experts sur des plates-formes technique
  - exercice de simulation de cyber-crise
    - entrainement de la cellule de crise

Et n'oubliez pas…

En savoir plus :
https://www.gouvernement.fr/info-coronavirus

MANIKA

Merci de votre écoute !

Lionel MOURER

lionel.mourer@manika-consulting.com

www.manika-consulting.com