AMUSEC
AIX-MARSEILLE CYBER SECURITY FORUM

Retour sur la cyberattaque du 14 Mars 2020 sur le SI de la mairie de Marseille

Jérôme POGGI / RSSI

VILLE DE MARSEILLE

Posons les bases

- Avant le 14 mars 2020
  - 2 salles serveurs en propre
  - +1200 serveurs
  - +6000 poste de travail répartis sur plus de 400 sites
- Le 14 mars 2020 ?
  - Un samedi après le vendredi 13
  - Le week end du premier tour des élections municipales
  - Dernier week-end avant le premier confinement

Le déroulé ...

Le 14 mars 2020

- 3h du matin - Perte de la téléphonie au standard Mairie
- 7h00 - Indisponibilité de certains services
  - Détectée par l'équipe réseau et serveur
- 7h31 - RSSI notifié pour évaluer « la panne » depuis Internet
  - VPN et Extranet indisponibles
  - Accès de secours opérationnel
- 8h15 → Quelque chose ne va pas !!!
- Entre 8h15 et 10h30 - analyse, tests, évaluation...
  - Vérifications physique sur site
  - Stade de pré-crise ...

Le 14 mars 2020

- 10h37 – Résignation et acceptation !
  - « Nous avons été compromis ! »
  - « Nos données ont été chiffrées ! »
- Déclenchement de la Crise
  - Les minutes et actions sont maintenant encore plus comptées
  - car « **ils** » sont encore là !
- 10h50 – « Bunkerisation » déclenchée
  - Terminée à 11h30
  - Coupure de TOUS les points d'interconnexions
    - Internet, partenaires, VPN, ADSL ...
  - Arrêt des stockages (en cours de chiffrement)
  - Arrêt des robots de sauvegarde (en cours d'effacement)

Le 14 mars 2020

- 11h30 – Mobilisation de la haute hiérarchie
  - Arrivée des premiers renforts techniques venus spontanément dès 9h
- 11h50 – Mobilisation/Réquisition de tout le personnel nécessaire
  - Mais pas de manière excessive … il faut ménager le personnel !
- 11h30 Lancement d'opérations en parallèle
  - Contacts extérieurs : ANSSI, Police, Métropole, partenaires..
  - Diagnostic → Besoin d'Expertise extérieure
  - Reconstruire d'un SI à minima → Expertise interne
- 12h - Destockage et re-installation d'un environnement virtuel basique
- 23h - Arrivée équipe « analyse post-incident » de Paris et fourniture des éléments demandés jusqu'à 3h
- Nuit très courte, la première d'une longue série ...

Les dégâts ...

Les dégâts

- Presque toute l'infrastructure virtuelle a été chiffrée
  - +800 serveurs et + de 90 To de données
- Sauf l'infrastructure segmentée, de sécurité et réseaux
- Une partie des sauvegardes a été chiffrée / effacée
- Notre NAS a commencé à être chiffré
  - Stoppé par nos actions rapide
- 80 % du SI détruit et le reste dans un état inconnu

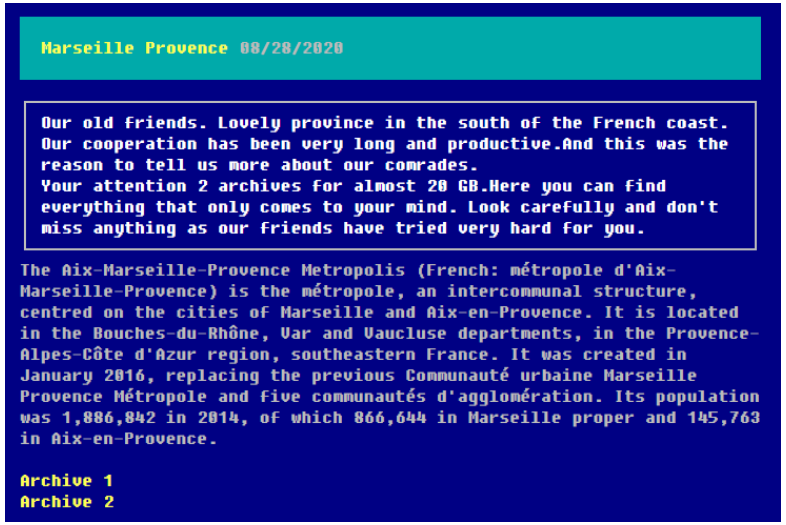
Actions clefs pendant la crise

Les actions clefs limitant la catastrophe

- Avoir gardé le calme et ne pas avoir paniqué
- Avoir cloisonné les réseaux
- Avoir mobilisé rapidement les équipes techniques
  - Les indices de compromission les plus critiques ont été trouvés par les agents de la DSI dans les 2 premières heures
- Avoir du personnel impliqué, compétent et expert
  - Infrastructure / sauvegarde / réseau / poste de travail / sécurité

Les actions clefs suivantes

- Contacter les autorités
  - Police/Gendarmerie, ANSSI, CNIL …
- Se faire aider
- Communiquer en interne et en externe
  - Juste mais pas trop
- Gérer la crise dans la longueur
  - Gestion RH, logistique …
  - 90 % du SI opérationnel après 6 mois
- Se préparer aux impacts de fuite d'informations
  - Le 28 août 2020 à 17h …



Et l’humain dans tout cela ?

L’humain dans tout cela ?

- Impact psychologique important
  - Épuisement, burn-out, lassitude, traumatisme
  - Cauchemars, insomnie, stress, perte de mémoire ...
  - Rarement prise en compte dans les procédure de crises
  - Plus long à arriver à identifier…
  - Sentiment de culpabilité, de faiblesse, de honte, peur de représailles / sanctions ...
  - Sur-crise …
- Nécessité d’un accompagnement psychologique !
  - C’est pour beaucoup un traumatisme

Conseils pour ne pas en arriver là ...

Conseils

- Se préparer à la Crise d'origine Cyber
  - Communication et organisation, exercices de crise
- Sécuriser son SI avant ...
  - Guide de sécurisation de l'ANSSI
- S'occuper sérieusement
  - des Sauvegardes,
  - Cartographie réseau, applicatif et interconnexions,
  - annuaire papier, base de mot de passe …
- Avoir une équipe « cyber » correct
  - Compétence, ETP en concordance avec les enjeux
- Plus l'attaque est complexe, plus les cyberdélinquants devront investir
  - But : devenir peu rentable pour les cyberdélinquants

Pièges à éviter lors d'une crise d'origine cyber

- Penser que payer la rançon permettra de redémarrer plus vite
- Rouvrir trop vite le système d'information
- Attendre un niveau de sécurité extrême avant de rouvrir
- Refuser un redémarrage en mode dégradé
- Vouloir tout redémarrer en même temps
- Mener des changements importants dans l'urgence

- Attendre la fin des investigations et le patient Zero pour lancer la reconstruction
- Ne pas anticiper la gestion des ressources humaines
- Cacher la situation aux agents, partenaires et citoyens
- Ne pas structurer le pilotage de la crise

VILLE DE MARSEILLE

AMUSEC AIX-MARSEILLE CYBER SECURITY FORUM

Existe-t-il une solution rapide et pas chère ?


Tous nos équipements sont 100% sécurisés
Nous les avons tous eteints !
Comment avez vous fait cela ?
© D.Fletcher for CloudTweaks.com

VILLE DE MARSEILLE

AMUSEC AIX-MARSEILLE CYBER SECURITY FORUM

Merci !