Témoignage cyberattaque La Rochelle
TRIP de printemps de l'Avicca

SECURITE DES SYSTEMES D'INFORMATION

Communauté d'Agglomération de La Rochelle

VILLE DE LA ROCHELLE

Introduction

Contexte : la Communauté d'agglomération et la Ville de La Rochelle ont mutualisé leurs directions des systèmes d'information le 1er janvier 2019.

Périmètre de la Direction des Systèmes d'Information Communs

3 000 postes de travail

400 serveurs

200 applications métiers

Les missions du Responsable de la Sécurité des Systèmes d'Information

- ✓ Créer et mettre en application la Politique de Sécurité des Systèmes d'Information
- ✓ Accompagner les métiers dans la formalisation des besoins de sécurité
- ✓ Former et sensibiliser les utilisateurs
- ✓ Homologuer les téléservices et les applications sensibles
- ✓ Contrôler le niveau de sécurité avec des tests d'intrusion

Témoignage : l'attaque

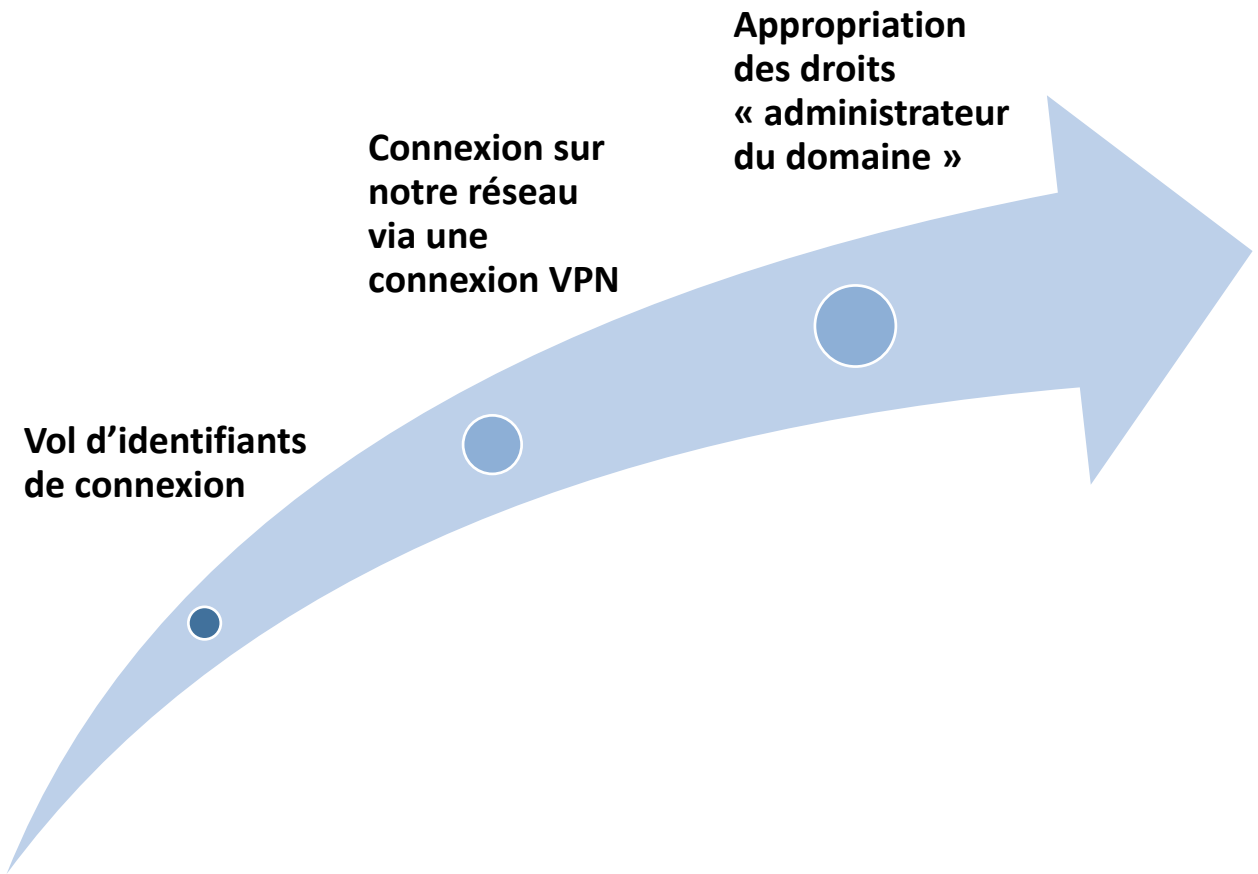
Samedi 26 décembre :
Attaque de 5h00 à 7h00 du matin

Dimanche 27 décembre :
Détection de l'attaque et extinction immédiate de tous les serveurs (VLR et CDA)

Lundi 28 décembre :
Cellule de crise pour gérer l'attaque

Mardi 29 décembre :
Rétablissement du SI de la CDA

Vendredi 22 janvier :
95% du système d'information VLR est de nouveau fonctionnel



Témoignage : les conséquences

Une attaque par rançongiciel pour une collectivité a un impact énorme sur ces valeurs essentielles :

- **Perte de la qualité du service public** :
  - L'ensemble des services était à l'arrêt ou en mode dégradé

- **Perte financière** :
  - Stationnement : en cette période, environ 6 000 euros / jour (rétablissement au bout de 4 jours)

- **Perte d'image** :
  - L'incident a été médiatisé à l'échelle nationale

- **Vol potentiel de données**

Témoignage : le plan d'actions

Suite à la cyberattaque, le plan de rétablissement s'est décomposé en trois phases :

1. **Investigation**
   - L'objectif est d'identifier les vulnérabilités exploitées par l'attaquant et de faire un état des lieux des ressources impactées. L'investigation a été menée par Orange Cyber Défense qui nous a accompagnés pendant 4 semaines. Le coût financier a été de 45 000 €.

2. **Restauration**
   - L'objectif est de rétablir les équipements informatiques permettant le bon fonctionnement de la collectivité (53/160 serveurs ont été restaurés et 42/900 ordinateurs ont été formatés)

3. **Sécurisation**
   - L'objectif est de sécuriser les vulnérabilités identifiées dans la phase d'investigation

Témoignage : durcissement de la sécurité

Quelques exemples de mesures de sécurité suite à la cyberattaque :

- ❑ Modification de tous les mots de passe (utilisateur, administrateur, équipements de sécurité…)
- ❑ Sécurisation du VPN (double authentification via certificat)
- ❑ Durcissement des équipements de sécurité
- ❑ Mise en place d'une sauvegarde déconnectée
- ❑ Création d'un Plan de Reprise d'Activité
- ❑ Veille quotidienne sur les failles de sécurité

Témoignage : bilan

Rétablissement rapide :
Le temps de rétablissement du système d'information de la Ville de La Rochelle a été très rapide (moins de 4 semaines)

Esprit de cohésion :
- Forte mobilisation de la DSIC : retour de vacances de certains collègues, soutien aux autres équipes, nombre important d'heures de travail
- Soutien de la hiérarchie : pas de pression et même une bienveillance de la part de la direction générale et des élus lors de la cyberattaque

Prise de conscience :
- Sensibilisation accélérée sur les risques de cyberattaque

Réflexion sur la mutualisation des Systèmes d'Information :
- Vigilance sur la mutualisation de deux systèmes d'information différents
  - Même niveau de sécurité sur les deux systèmes d'information
  - Penser au cloisonnement de certains périmètres non mutualisables

Contacts

Denis Vermot
Directeur des Systèmes d'Information Communs

Denis.vermot@agglo-larochelle.fr

Mathieu Souchard
Responsable de la Sécurité des Systèmes d'Information

Mathieu.souchard@agglo-larochelle.fr
05 46 37 73 29