DCSI

Sécurité du Système d'Information

Ordre du jour

- Historique et Point de situation
- Bilans et Actions à venir
- Conclusions

Historique

Préambule :
Système d'Information mutualisé entre l'Agglo et les 2 Villes centres/CCAS depuis 2016

Contexte :

- Cybercriminalité en forte croissance depuis plusieurs années
- Réglementations étoffées (RGPD, Loi Programmation Militaire, NIS 1 et 2)

➔Nécessité d'améliorer notre SI en matière de sécurité

Historique

Responsable Sécurité du SI (½ ETP) nommé fin 2018 rattaché au DSI

Missions :

- Définir la stratégie en matière de cybersécurité
- Etablir une feuille de route pour améliorer de niveau de sécurité du SI

Historique

Opportunité du Plan France Relance 2020 :

→Parfaire l'état des lieux en matière de cybersécurité du SI

→Permettre de conforter les 1ères orientations, et d'accélérer et compléter le plan d'actions à mener

Engagement sur plan d'actions sur 3 ans pour bénéficier de la subvention du Pack Relais Initial

Historique

3 types d'actions identifiées :

- Technique
- Organisationnel/Gouvernance
- Sensibilisation/Formation (prise de conscience à tous les niveaux, bonnes pratiques, …)

Bilans

En termes financier :

Pack relais initial :

73 k€ TTC d'investissement (Subv ANSSI 50 k€ TTC)

En matière de charge humaine depuis 2021 :

1,5 à 2 ETP

(RSSI, pilotage projets acquisition solutions SSI, impacts des actions à mener autour de la sécurité (supervision, travaux contre vulnérabilités, ...))

Bilans

Objectifs d'évolution de l'indice de cybersécurité et du scoring ANSSI dans le cadre du Plan de relance

Au Début du Plan	Après Plan Initial (3 ans)	Après Plan de Relance (5 ans)
INDICE DE CYBERSECURITE		
C-	C+	B-
SCORING		
3,8	4,6	6,4

L'indice de Cybersécurité pour les collectivités similaires était D+ (scoring =~3)

Bilans

Indicateurs ont beaucoup évolué en 5 ans (indicateurs à l'origine ne sont plus pertinents à suivre, et les plus récents sont mis en place depuis trop peu de temps donc peu de recul)

→ Comparaison impossible depuis le début du Plan

Bilans

Sites applicatifs exposés à l'extérieur :
65 000 tentatives d'attaques bloquées / mois

Messagerie :
- Entre 600 000 et 1 000 000 mails reçus /mois
- Blocage : ~54% spam, 1% virus et autres malwares

Vulnérabilités SI (un peu plus technique):
>140 000 vulnérabilités corrigés sur 2024 réduisant la « surface d'attaque »
Amélioration de 30% de la protection de l'annuaire technique (élément névralgique du SI)

Bilans

Quelques exemples particuliers :

Contraignants mais positif en termes de sécurité

- Filtrage internet

→ Empêche les accès à des sites inappropriés ou dangereux (dont plateformes de téléchargement)

- « Segmentation réseau »

→ Limite le propagation des éventuelles attaques

- « Portail d'accès aux prestataires informatiques »

→ Sécurise les accès extérieurs

- Complexification et diminution de la période de validité des mots de passe

→ Réduit les risques de piratage de comptes

Bilans

Focus sur l'accompagnement auprès des agents :

- Actions multiples autour de la gestion des mots de passe
- Sensibilisation :
  - Montée en compétence des agents sur des notions informatiques
  - Indication sur les bonnes pratiques à adopter en matière de mails, de navigation internet, …
- Campagnes de faux-phishings pour mesurer l'adoption des bonnes pratiques et identifier les actions de sensibilisation ciblées
- Signature Charte utilisateur

Actions à venir

Poursuivre les actions identifiées dans le plan d'actions

Répondre aux nouvelles exigences réglementaires (transposition NIS 2 – application au 18/10)

- Renforcement du niveau de sécurité autour des SI des Entités Essentielles et Importantes (Eau potable, Eaux Usées, Energie, Gestion des Déchets, Infrastructures Numériques,) pour collectivités > 30 k hab
- A priori 3 ans pour mise en conformité

Actions à venir

En termes financier :

Estimation investissement :

25 à 75 k€ TTC/an (sans NIS 2)

Estimation fonctionnement :

100 à 150 k€ TTC/an (sans NIS 2)

En matière de charge humaine :

2 à 2,5 ETP

(RSSI, pilotage projets acquisition solutions SSI (au moins 3 ans), impacts des actions à mener autour de la sécurité (supervision, travaux contre vulnérabilités, ...))

Conclusions

Démarche lancée il y a 5 ans, qui après 2 ans a pu être « accélérée » par le Plan de Relance : aide financière et accompagnement pour disposer de la complétude des éléments

Impacts en termes de budget d'investissement et de fonctionnement important (à long terme), et de charge humaine très significative (sur la partie technique comme sur l'accompagnement des utilisateurs)

Conclusions

Amélioration significative du niveau de Cybersécurité du SI, mais il reste de nombreux chantiers

Indispensable face aux risques encourus :
10% des collectivités ont été attaquées sur l'année écoulée avec des impacts de plus en plus significatifs (40% d'interruption de services/activités, 20% perte de données, 20% perte financière)