CE Alsace

Transformation numérique / RH

Sensibiliser aux cybermenaces

Le problème

Les collectivités locales font face à une augmentation alarmante des cyberattaques, permise par une vulnérabilité accrue due à la numérisation croissante de leurs services et à la sophistication des cybercriminels. L'humain est souvent le maillon faible dans cette chaîne de sécurité, exposant les systèmes à des risques majeurs tels que l'hameçonnage (l'attaque la plus répandue) et les rançongiciels.

Votre solution innovante

La CeA a développé une stratégie de cybersécurité centrée sur la sensibilisation, la formation continue et l'adoption de bonnes pratiques pour tous les agents et les élus, en les transformant en défenseurs actifs contre les cybermenaces.

Les objectifs

- Informer et sensibiliser tous les agents et élus sur les risques associés aux cybermenaces, ainsi que sur les bonnes pratiques en matière de cybersécurité.
- Diminuer le nombre d'incidents de cybersécurité dus à des erreurs humaines.

L'histoire de votre action innovante

- ***Qui ?***

L'équipe en charge de la cybersécurité, la direction générale ainsi que la Direction des Systèmes d'Information et du numérique. Avec un prestataire extérieur.

- ***Pour qui ?***

Tous les agents et élus de la CeA, ainsi que les partenaires impliqués dans les opérations numériques.

- ***Quoi ?***

La Collectivité européenne d'Alsace a mis en œuvre une stratégie de sensibilisation par des actions visant à développer une culture de cybersécurité solide et cohérente au sein de la CeA, en impliquant activement agents et élus.

Trois piliers fondamentaux : sensibilisation, formation et communication.

- Cyberlois en octobre : participation annuelle à l'initiative européenne pour sensibiliser aux cybermenaces, avec focus sur la lutte contre les fraudes par ingénierie sociale en 2023.
- Ateliers de sensibilisation : ateliers en ligne pour former les agents aux bonnes pratiques de cybersécurité et comprendre les méthodes des cybercriminels.
- Parcours de formation en ligne : sessions courtes et accessibles pour acquérir les bases de la cybersécurité, avec un programme de sensibilisation couvrant six thématiques annuelles. Partenariat avec un prestataire pour des contenus interactifs et ludiques, incluant vidéo, quiz et fiches thématiques.
- Cyberchallenge
- Charte de cybersécurité : adoption d'une charte définissant les règles et comportements attendus pour sécuriser les systèmes d'information et les données.
- Formation des Élus : pour sensibiliser les élus aux dangers cyber et les préparer à répondre efficacement en session du Conseil d'Alsace, programmes spécifiques couvrant : la protection des données personnelles (RGPD), la sécurisation des systèmes d'information, les risques cyber et les responsabilités juridiques.

- ***Quand ?***

2021 : définition de la Politique de Sécurité des Systèmes d'Information ; la sensibilisation constitue l'un des trois piliers de la politique
Puis déploiement des outils de sensibilisation quotidienne

- Lancement du Cybermois : diffusion de vidéos de sensibilisation, quiz interactifs, ateliers de sensibilisation en ligne sur la cybersécurité pour tous les agents.
- Développement des modules de formation en ligne et création de la charte cyber.
- Lancement des programmes de formation pour les élus et les maires du Bas-Rhin

Suivi et évaluation des résultats de la stratégie de sensibilisation et de formation.
Exercices de simulation d'incidents pour tester la préparation et la réponse.

Les moyens humains et financiers

Une partie de la sensibilisation est exécutée en interne, la plateforme d'apprentissage et de sensibilisation représente un coût de 20 à 30 000 euros par an.

L'évaluation de l'innovation

- ***Impact***

Plus de 65% des agents ont participé aux modules mensuels.
Réduction du taux de clic sur des liens malveillants et diminution des incidents liés à des actions malveillantes comme les *phishing*, grâce à la sensibilisation accrue : baisse de plus de 20% dans les campagnes et signalement beaucoup plus nombreux de la part des agents.

- ***Potentiel de diffusion et de réplication***

Présentation du projet dans des conférences sur la cybersécurité et partage avec d'autres collectivités.

- ***Bilan, suivi, projet d'évolution***

Plusieurs fois dans l'année des campagnes-tests permettent de mesurer si les agents cliquent sur les liens voire s'ils indiquent leur mot de passe : faux-mails de phishing, par exemple faux mail de sécurité sociale. En dépit de campagnes de plus en plus sophistiquées, le taux de clics baisse (même s'il constitue un risque encore important).
Projet d'évolution :

- Ajouter des modules de formation régulièrement mis à jour pour tenir compte des nouvelles menaces et technologies émergentes.
- Adopter une approche d'amélioration continue pour intégrer de nouvelles pratiques et technologies émergentes pour renforcer notre posture de cybersécurité.

Mots-clés : Cybersécurité / Sensibilisation / Formation