Procédure en cas de cyberattaque ou violation de la sécurité des données pour l'administration communale d'Attalens

Cette procédure a pour but de réagir correctement à des événements inattendus et assurer la continuité des opérations communales.

Ce document s'adresse à tout le personnel utilisant l'infrastructure informatique de la Commune d'Attalens.

Version du 13.11.2023

Doc sous \\192.168.20.21\Data\0_AdminGen\022_SecGen\0220_SecGen\0220.04_IT\.03_PrestatLogiciels\Divers

Etapes et actions	**Qui**
1. Identification de l'incident	
• Si détection ou soupçon d'une cyberattaque ou de violation de la sécurité des données, informer immédiatement l'administrateur communal (021 947 33 75) ou remplaçant (chef du service technique 021 947 55 71) et le prestataire informatique (VG Technologies 021 943 50 50).	impliqué.e
• Documenter toutes les observations pertinentes, y compris l'heure exacte, la nature de l'incident et les systèmes potentiellement affectés. Si possible avec des photos ou saisies d'écran.	impliqué.e
2. Isolation de l'incident	
• D'entente avec le prestataire informatique, déconnecter les systèmes compromis du réseau pour éviter une propagation ultérieure, éteindre l'ordinateur, retirer la prise réseau de la machine.	impliqué.e + prestataire informatique
• Changer les mots de passe pour tous les comptes utilisateurs et administrateurs sur les systèmes affectés.	impliqué.e + prestataire informatique

projet

3. Notification aux parties concernées	
• Informer le syndic, le Conseil communal et les autres parties prenantes de la situation.	administrateur communal
• Si des données personnelles ou sensibles ont été compromises, informer les autorités compétentes conformément à la réglementation en vigueur (police)t annoncer à l'Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM via le formulaire en ligne	administrateur communal
• Au besoin, mettre en place une cellule de crise avec le syndic, l'administrateur et le prestataire informatique.	administrateur communal
4. Évaluation et analyse	
• Rassembler les journaux et les données pertinentes pour évaluer la nature et l'ampleur de l'incident.	prestataire informatique
• Utiliser des outils de diagnostic et de surveillance pour identifier la source et la méthode d'attaque.	prestataire informatique
5. Éradication	
• Une fois la source de l'incident identifiée, supprimer tous les éléments nuisibles.	prestataire informatique
• S'assurez d'avoir corrigé toutes les vulnérabilités qui ont permis l'attaque.	prestataire informatique
6. Restauration	
• Restaurer les systèmes à partir de sauvegardes connues pour être propres et sûres.	prestataire informatique
• Mettre à jour et patcher tous les logiciels et systèmes pour prévenir des incidents futurs.	prestataire informatique
7. Communication	
• Si nécessaire, préparer un communiqué pour informer le public, les résidents et autres parties prenantes de la situation, des mesures prises et des recommandations pour éviter d'autres incidents.	syndic + administrateur communal
• S'assurer de répondre aux questions et préoccupations de manière transparente et ouverte.	syndic + administrateur communal
8. Revue post-incident	
• Organiser une réunion avec toutes les parties impliquées pour discuter de l'incident, des mesures prises et des leçons apprises.	administrateur communal

projet