

La solution de sauvegarde Atempo permet de redémarrer les services de la Mairie

ee

« La solution Continuity est comme une boîte noire sécurisée et déconnectée. C'est très rassurant pour nous d'avoir sur site, une sauvegarde des données sur un serveur déconnecté du domaine et intouchable par des attaques. »

99

DSI, Mairie de +50 000 habitants

LE CHALLENGE

La mairie, qui souhaite rester anonyme pour des raisons de sécurité, fait partie des collectivités territoriales dont la mission principale est d'assurer la gestion quotidienne de plus de 50 000 administrés.

L'infrastructure informatique de la mairie compte **environ 500 postes de travail, plusieurs dizaines de serveurs et applications métiers**, représentant une volumétrie de données de **plus de 50 To**.

Pour garantir la **continuité de son activité**, l'équipe informatique, composée de 7 personnes, a déploie une solution de sauvegarde des serveurs, avec un **PRA (Plan de Reprise d'Activité)** en cas de crash ou de perte de données.

En complément de sa solution existante, l'équipe informatique recherche une solution de sauvegarde secondaire déconnectée du domaine, afin de maintenir la **continuité du service public**.

LA SOLUTION

Continuity Premium, la solution de **confiance** d'Atempo, a été choisie pour assurer la **sauvegarde sécurisée** des données de la mairie **sur site**, via une appliance déconnectée.

« Les solutions souveraines d'Atempo sont labellisées **'Utilisé par les Armées Françaises'**. Pour nous, cela représente un gage supplémentaire de qualité et de fiabilité. »

Jour J 00h10 : Cyberattaque

La Mairie a été la cible d'une attaque de type rançongiciel.

Attaque par chiffrement

Une rançon d'un million d'Euros a été demandée pour récupérer les clés de chiffrement et pour la non-divulgaration des données.

Rançon refusée par la mairie

« Un maximum de données ont été chiffrées très rapidement. »

J+1 08h20 : Arrêt total et analyse de la situation

L'intégralité des serveurs a été chiffrée : fichiers, bases de données (Oracle, SQL), téléphonie, sauvegardes.

Rien n'a été épargné

« C'est là que nous nous sommes rendu compte que la solution de sauvegarde principale était compromise et inopérante face aux attaques par chiffrement. »

J+2 06h00 : Début de la restauration

La restauration des systèmes se fait progressivement : d'abord la téléphonie puis certaines applications cloud.

80% des serveurs à nouveau opérationnels.

« Nous avons mis seulement quelques jours pour redémarrer les serveurs sauvegardés par Continuity. »

ee

« Les serveurs restaurés ont été passés au peigne fin pour vérifier leur intégrité, puis nous avons procédé à une refonte complète de l'active directory. »

Directeur des Systèmes d'Information, Mairie de +50 000 habitants

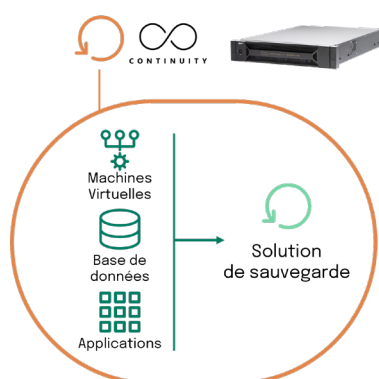
99

LA CYBER RÉSILIENCE

Face à de telles situations de crise, l'équipe informatique a su faire preuve d'une grande réactivité en appliquant les dispositifs de remédiation suivants :

- 1. Se déconnecter** : les accès à toutes les sources (WAN) ont été coupés, afin d'isoler le système affecté et empêcher la propagation de l'attaque. La rapidité de l'intervention a permis de limiter le volume de données chiffrées.
- 2. Déposer plainte auprès des autorités compétentes** : l'attaque a été immédiatement signalée, avec l'accompagnement de l'ANSSI.
- 3. Fédérer les équipes en interne et les forces vives extérieures** : cette étape est primordiale pour garantir la bonne coordination et la prise de décision.
- 4. Identifier et corriger la faille** : une passerelle laissée ouverte a permis d'identifier le point d'entrée de l'attaque.
- 5. Récupérer les données chiffrées** : l'intégrité des sauvegardes d'Atempo a été préservée, permettant de redémarrer les serveurs.

« Nous sommes restés dans le noir pendant 11 jours, au lieu des 2 à 6 mois généralement constatés, et grâce aux systèmes de sauvegarde Continuity d'Atempo, décorrélés du domaine, l'intégralité des données a pu être restaurée rapidement. »



Pour rappel, à la suite d'une attaque par chiffrement, le délai moyen de remédiation est de **deux mois**, et peut atteindre six mois pour des attaques de grandes ampleurs sur des systèmes non préparés (source : Sophos).

Pour conclure, le DSI souligne **l'importance cruciale de disposer de systèmes de sauvegarde immuables**. À l'avenir, la mairie envisage de renforcer davantage la protection de ses données en **externalisant une copie de sauvegarde en dehors de l'hôtel de ville**.

LES BÉNÉFICES MÉTIER



Solution sécurisée,
non-visible sur le domaine



Possibilité de réplique
des données sauvegardées



Rapidité des restaurations
pour relancer les serveurs

Consulter la fiche produit



<https://links.atempo.com/DP-presentation>

Contacter un expert Atempo



<https://links.atempo.com/continuity-contact>

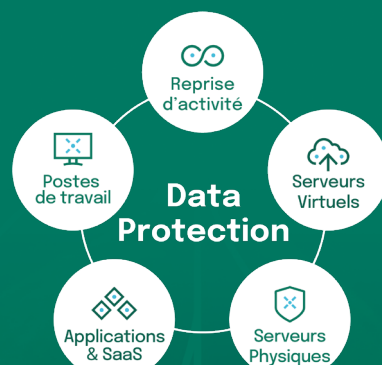
Mise à jour : 09/01/2024

POWERFUL DATA PROTECTION AND DATA MANAGEMENT SOLUTIONS - atempo.com

Atempo Headquarters | 23, Avenue Carnot, 91300 Massy, France | Tel: +33 164 868 300 | info@atempo.com

LES BÉNÉFICES

- Solution de **confiance**, **100% française**
- Solution **labellisée 'Utilisée par les Armées Françaises'**
- Sauvegarde **automatisée et en continu**
- Données **dédupliquées et compressées**
- Authentification forte**
- Tarification claire** sans coût caché
- Protection** du système de sauvegarde existant



CONTINUITY

