Retour d'expérience

PIRATAGE DE MESSAGERIE

La Mission numérique du PETR du Pays Auxois Morvan, conjointement avec Cybergogne, vous propose ce retour d'expérience partagé suite à une compromission de messagerie visant une commune de l'Auxois Morvan.

Illustration ©Adobe Firefly 2026

Pour une commune rurale, la messagerie électronique est le pilier de la vie numérique de la collectivité. Elle permet l'échange avec les administrés, les autorités et les partenaires locaux ainsi qu'avec les acteurs associatifs ou économiques du territoire. Ce retour d'expérience explicite les risques d'une faible sécurité de la messagerie et propose des solutions pour la renforcer.

SITUATION

La commune, qui consulte sa messagerie en ligne sur le site web d'Orange, constate que des courriels disparaissent et que des contacts du carnet d'adresses sont modifiés. Elle en conclut rapidement qu'un accès frauduleux est en cours.

QUELLES SONT LES CONSÉQUENCES D'UN ACCÈS FRAUDULEUX ?

De par l'importance de la messagerie électronique dans la gestion d'une commune, la compromission de celle-ci génère des conséquences multiples :

1. l'usurpation d'identité, à des fins d'escroquerie, de scams, d'accès à d'autres services numériques etc.
2. la fuite de données à caractère personnel : la messagerie d'une commune conserve de nombreux échanges et informations avec les administrés, informations qui peuvent être préjudiciables en cas d'utilisation malveillante.
3. la perte de confiance des administrés : les nombreuses fuites de données impactant les grandes sociétés ou entités publiques pénalisent la confiance des utilisateurs dans les outils numériques.
4. des conséquences juridiques pour le maire, qui peut voir sa responsabilité engagée au titre du défaut de sécurisation de l'informatique communale.

QUELLES FAILLES A-T-IL PU EXPLOITER ?

Pour se connecter en toute discrétion à la messagerie de la commune, l'attaquant a tiré profit de l'absence des mesures de sécurité suivantes :

- **faiblesse du mot de passe** pour se connecter à la messagerie ;
- **absence de double authentification**, aucun avertissement ne pouvait signaler des tentatives de connexion ;
- **concentration des données dans la messagerie** : la messagerie conserve de nombreux documents exploitables par l'attaquant.

QUELLES DONNÉES L'ATTAQUANT A-T-IL PU RASSEMBLER ?

En parcourant la messagerie, l'attaquant a pris connaissance de nombreuses informations à caractère personnel ; on peut identifier les types de documents suivants :

- devis, factures (nom de prestataires, travaux demandés, montant des travaux...),
- actes notariés, document de propriété, héritage (accès à des documents confidentiels),
- **informations bancaires diverses**, RIB, mouvements bancaires (habitudes d'achat, capacité d'investissement etc.),
- signatures dématérialisées, cachets, sceaux (facilitent la création de faux documents),
- informations d'ingénierie sociale sur l'équipe municipale (multiplient les chances de répliquer l'attaque et augmentent les chances de réussite),
- **échanges de courriels relatifs aux affaires de la commune**.

Les différentes versions numériques de ces documents permettent à l'attaquant de concevoir des faux réalistes et crédibles.

COMMENT SÉCURISER L'ENVIRONNEMENT NUMÉRIQUE ?

- **Adopter un mot de passe de messagerie robuste et unique**, en s'appuyant sur un coffre-fort numérique ;
- Abandonner la messagerie gratuite Orange (ou Wanadoo) proposée avec l'accès à Internet. L'absence de double authentification robuste ne permet pas de sécuriser la messagerie de la commune. La collectivité a intérêt à se tourner vers une offre professionnelle robuste, qu'elle émane de prestataires privés ou de prestataires publics comme l'ARNia.
- **activer la double authentification lorsqu'elle est proposée**,
- passer en revue les règles de transfert automatique des courriels ;
- passer en revue les autorisations pour les applications tierces : **mettre en place un mot de passe d'application** pour sécuriser l'accès à chacune.

Et plus généralement :

- appliquer les mises à jour des logiciels lorsqu'elles sont publiées,
- supprimer les logiciels non utilisés ou obsolètes,
- s'astreindre à une sauvegarde efficace ou opter pour un service de sauvegarde fourni par un prestataire privé ou public.

LE DÉPÔT DE PLAINTE

Dès que l'attaque est constatée, il est important de réagir au plus vite. En effet, selon la portée de l'attaque, un compte à rebours peut s'appliquer : dans le cas d'une fuite de données à caractère personnel, la collectivité devra contacter la CNIL dans un délai de 72h.

Concernant les communes et les collectivités, la Gendarmerie ou le commissariat doivent recueillir la plainte : il faudra alors fournir des justificatifs (captures d'écran, impressions, photos).

Ces preuves pourront également être présentées à l'assurance de la commune : en anticipation de crise, il est intéressant de solliciter son assureur pour comprendre quels sont les services proposés par celui-ci en termes de risques numériques.

Ce retour d'expérience a été rédigé d'après l'analyse post-mortem fournie par Cybergogne.

CYBERGOGNE

La sécurité en toute transparence

CYBERGOGNE

Solutions de cybersécurité adaptées aux petites collectivités et aux TPE/PME en Bourgogne

- Diagnostic / plan d'actions / durcissement
- Sensibilisation (agents & élus)
- Appui en cas d'incident (en lien avec l'écosystème régional)

CONTACT (pour ce retour d'expérience)
Michel Ract-Mugnerot – Architecte Cloud & Sécurité
Tél. : **+33 6 15 28 14 35**
Web : **https://www.cybergogne.fr**
Adresse : 3, place de l'Église
21210 Saint-Martin-de-la-Mer (France)

En cas d'attaque, contactez le centre de réponse à incident cyber :
CSIRT BFC au 0 970 609 909

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

LES INDISPENSABLES DE LA SÉCURISATION

Gestionnaire de mots de passe : le gestionnaire de mots de passe est un logiciel qui permet de créer, conserver et partager des mots de passe robustes. Concernant la création, le gestionnaire respecte les contraintes de variété des suivantes : lettres minuscules et majuscules, chiffres, caractères spéciaux, longueur minimum. Il mémorise les mots de passe dans une base de données chiffrée, protégée par un mot de passe principal. Enfin, il permet le partage, entre ordinateurs, téléphones portables et personnes autorisées.

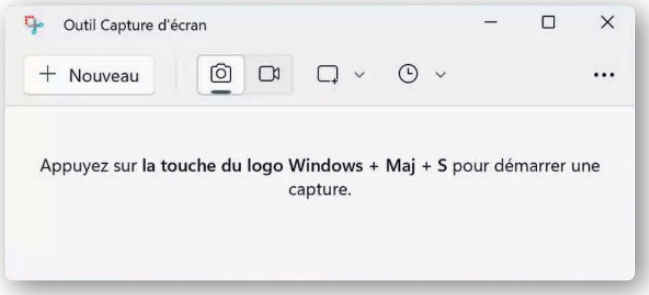
Double authentification, MFA, OTP : la double authentification (2FA), l'authentification multi-facteur (MFA) ou le recours au mot de passe unique (OTP) sont des procédés de vérification pour les connexions. Complémentaire au mot de passe, la double authentification permet de vérifier que la personne se connectant à un service est bien celle autorisée initialement à le faire. Dans la majorité des cas, la vérification s'effectue au moyen d'un téléphone portable.

Retour d'expérience
FICHE RÉFLEXES

La Mission numérique du PETR du Pays Auxois Morvan, conjointement avec Cybergogne, vous propose cette fiche réflexes. Vous retrouverez différentes aides et solutions pour savoir comment réagir face à une cybermenace.

Quelles preuves conserver ?

1) **Captures d'écrans, photographies de l'écran** : ciblez l'écran dans son intégralité, pas seulement une partie ou la fenêtre en cours ;
2) **Enregistrements audio** : certains téléphones portables permettant d'enregistrer les conversations ;
3) **Historique des connexions internet** : les navigateurs conservent la succession des pages visitées ;
4) **Historique des appels téléphoniques** : numéros, temps de conversation, dates ;
5) **D'autres éléments peuvent servir de preuves** : il faudra alors solliciter un professionnel pour les identifier et les exploiter.



Le RGPD en 6 lignes

1) Ne collectez que les **informations strictement nécessaires** (cela réduit les impacts des fuites de données) ;
2) **Soyez transparent** : les personnes concernées doivent être informées ;
3) Les personnes doivent **pouvoir exercer facilement leur droit** de consultation ou d'accès, de rectification ou de suppression des données qui les concernent ;
4) Définissez des **durées de conservation réalistes**, puis détruisez, anonymisez ou archivez les données collectées, selon les obligations légales ;
5) Anticipez les risques et **sécurisez les données** ;
6) Suivez attentivement votre mise en conformité en **réexaminant régulièrement** les éléments ci-dessus.

Qui contacter en cas de compromission ?

Selon la nature de la compromission, vous devrez contacter différents organismes. Les propositions ci-dessous correspondent aux contacts à solliciter dans la majorité des cas. Avant tout incident, élaborez, à tête reposée, votre liste de **contacts vérifiés** : sous la pression d'une cybermenace, vous pourrez vous appuyer sur ce document.

1) Notez le jour et l'heure où vous avez constaté la compromission ;
2) Contactez votre prestataire ou référent informatique si vous en avez un ;
3) Alertez le Centre de Réponse à Incident Cyber au 0 970 609 909 suivi du choix 1 ;
4) Alertez également la Gendarmerie ;
5) Alertez la Trésorerie ou votre Banque, s'il y a une suspicion de transferts de fonds ;
6) Déposez plainte ;
7) Dans les 72 heures (voir point 1), vous devrez :
   A. déclarer le sinistre à votre assureur ;
   B. notifier la CNIL si des données à caractère personnel ont pu être consultées, modifiées ou détruites.
8) Informez les contacts qui peuvent être impactés par la compromission : il peut s'agir d'administrés, de fournisseurs, de partenaires ou de toute personne dont la sécurité est compromise par l'incident.

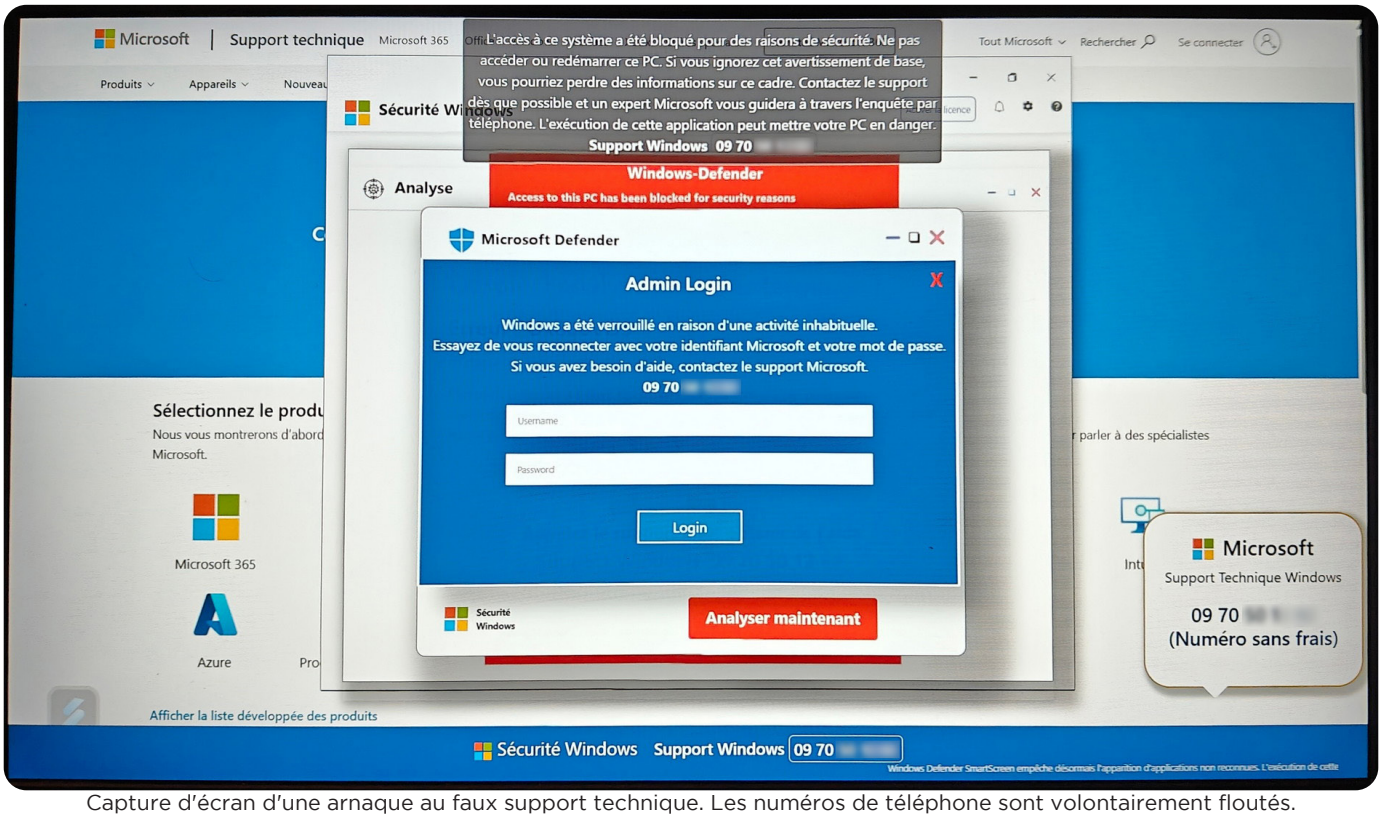
URGENCE :
isolez la machine incrimée du réseau

Dès la compromission constatée, débranchez l'équipement concerné du réseau. Débranchez la prise réseau (RJ-45) et vérifiez que l'appareil n'a pas basculé en Wi-Fi.
Évitez de l'éteindre, branchez-le sur secteur s'il s'agit d'un équipement portable.

Exemple de « scareware » - arnaque au faux support technique

Urgence et menace
Le message occupe tout l'écran prétendant que l'ordinateur est bloqué.
Objectif : provoquer la panique, forcer à agir dans l'urgence

Usurpation de l'identité visuelle de Microsoft Windows
Les icones, textes et couleurs simulent un message de l'ordinateur, invitant à appeler un numéro.
Ce n'est pas le canal officiel : c'est l'arnaque



Capture d'écran d'une arnaque au faux support technique. Les numéros de téléphone sont volontairement floutés.

Vol d'accès et prise de contrôle
Faux écran de connexion administrateur : l'attaquant force la victime à transmettre son identifiant et mot de passe pour obtenir les droits sur la machine (accès à la messagerie, outils métiers etc.)

Réflexe immédiat (élus, agents)
- Conserver une capture d'écran et noter l'heure ;
- Fermer la page (raccourci clavier ALT+F4) ;
- Contacter un référent ou un prestataire informatique ;
- Ne pas appeler le numéro affiché par les escrocs !

CYBERGOGNE
La sécurité en toute transparence

En cas d'attaque, contactez le centre de réponse à incident cyber :
CSIRT BFC au 0 970 609 909

CYBERGOGNE
Solutions de cybersécurité adaptées aux petites collectivités et aux TPE/PME en Bourgogne
• Diagnostic / plan d'actions / durcissement
• Sensibilisation (agents & élus)
• Appui en cas d'incident (en lien avec l'écosystème régional)

CONTACT (pour ce retour d'expérience)
Michel Ract-Mugnerot – Architecte Cloud & Sécurité
Tél. : **+33 6 15 28 14 35**
Web : **https://www.cybergogne.fr**
Adresse : 3, place de l'Église
21210 Saint-Martin-de-la-Mer (France)

CSIRT
BOURGOGNE-FRANCHE-COMTÉ