AU CŒUR
DU DÉBAT PUBLIC

COMMISSION
NUMÉRIQUE

LA SÉCURITÉ NUMÉRIQUE DES COLLECTIVITÉS TERRITORIALES

COMMENT SE PROTEGER FACE AUX CYBERATTAQUES ?

Compte-rendu de la séance du 01/02/2022

I INTERVENANTS

Julien Chambon, Maire de la Commune de Houilles (78)

Guillaume Crepin, Délégué régional de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

David Prache, Dirigeant et cofondateur de la startup de coaching en cybersécurité OPPENS – Groupe Société Générale

Laurent Verdier, Chargé de mission sensibilisation – risque cyber pour le Groupement d'Intérêt Public Action contre la Cyber-malveillance (GIP ACYMA)

Le mardi 1er février 2022 de 9h00 à 11h

En visioconférence

Élus référents :

- **Eddie Aït**, maire de Carrières-sous-Poissy (78)
- **Christophe Ippolito**, adjoint au maire de Nogent-sur-Marne (94)
- **Dominique Turpin**, maire de Nézel (78)

CONTEXTE

L'année 2020 a été marquée par un grand nombre de cyber-attaques envers les collectivités locales. En effet, les signalements d'attaques par rançongiciels[1] ont été multipliés par 3 entre 2019 et 2020. Ces signalements émanaient autant de grandes collectivités que des plus petites. Au total, près de 30% des collectivités en France ont déjà été victimes de l'un de ces rançongiciels.

Selon une table-ronde sénatoriale sur la cybersécurité, quatre motifs expliqueraient la banalisation de ce type de cyberattaques :

- La numérisation de l'économie et des services publics, accélérée avec le confinement lié au développement du télétravail et le déploiement de la fibre
- La professionnalisation de la cybercriminalité, facilitée par sa « plateformisation », son industrialisation, et le développement des cryptomonnaies ;
- La difficulté de la prévention et de la répression, lesquelles nécessitent à la fois la prise de conscience de tous et une coopération internationale efficiente ;
- L'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique dont les collectivités territoriales, leurs établissements publics et les établissements de santé, sont soit les cibles soit les victimes collatérales.

Une prise de conscience collective s'est faite que toutes les collectivités publiques

[1] Selon Cybermalveillance.gouv.fr : un rançongiciel est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès

pouvaient être des cibles potentielles, y compris les plus petites. Ces petites communes sont d'ailleurs bien souvent démunies et moins bien armées numériquement face aux attaques.

Une commune de 5 000 habitants, qui a témoigné anonymement pour Cyber-malveillance, a expliqué avoir subi un piratage du site internet de sa collectivité en raison des failles de sécurité liées à une non mise à jour du site. Plusieurs semaines furent nécessaires au rétablissement de l'ensemble des services de la collectivité.

Cette vigilance face aux vulnérabilités des systèmes d'information se trouve d'autant plus mise en avant par les acteurs de la cybersécurité dans le contexte de la tenue des scrutins présidentiel et législatifs de 2022.

Une note produite par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)[2] rappelle plusieurs bonnes pratiques à adopter quotidiennement pour se prémunir face à ces attaques de rançongiciels, parmi lesquelles la sauvegarde régulière des données sur des supports hors ligne, la mise en place de mots de passe complexes et uniques et une vigilance accrue sur les pièces-jointes pouvant sembler douteuses.

Les sujets liés à la sécurité numérique des systèmes d'information (SI) peuvent être difficiles à s'approprier par les élus locaux, du point de vue de la technicité de certains outils informatiques.
Néanmoins, l'élu a un rôle déterminant à jouer auprès de ses agents et de ses administrés pour :

- Impulser un effort collectif (former et sensibiliser ses collaborateurs, allouer des investissements à la sécurisation du numérique)
- Forger une vision globale et définir des priorités d'action (faire un état des lieux de sa collectivité, cartographier les systèmes d'information)
- Préparer la collectivité à agir face à une situation de crise (lister les contacts clefs, préparer une communication de crise, connaître les principales obligations juridiques)

[2] Consultable à l'adresse suivante : https://www.cher.gouv.fr/content/download/31532/209786/file/20211217_np_anssi_plaquette_scrutins_2022_v1h.pdf

Les acteurs de la cybersécurité en France :

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) :

Autorité nationale en matière de sécurité des systèmes d'information créée par décret en 2009, l'Agence est placée sous l'autorité du Premier ministre et est rattachée au secrétaire général de la défense et de la sécurité nationale.

A ce titre, l'ANSSI :

- Coordonne l'action gouvernementale en matière de défense des systèmes d'information à l'échelle nationale
- Elabore les mesures de protection des systèmes d'information et veille à leurs applications
- Se prononce sur la sécurité des dispositifs de protection des systèmes d'information et des prestataires de services de confiance

Le Groupement d'Intérêt Public Action contre la Cyber-malveillance (GIP ACYMA)

Le GIP ACYMA est la structure chargée de piloter la plateforme *Cybermalveillance.gouv.fr.* Elle est chargée de sensibiliser, de prévenir et d'aider les victimes de cyber-malveillance, que ce soit auprès des particuliers, des entreprises ou des collectivités. En tant que groupement d'intérêt public, le GIP ACYMA adopte une gouvernance partagée par un collège d'acteurs publics (Ministères, Agence d'Etat, collectivités, etc…) et privés (Orange, Google, Microsoft, Bouygues, etc…)

A ce titre, le GIP ACYMA :

- Assiste les victimes d'actes de cyber-malveillance
- Mène des actions de prévention des risques à la cybersécurité
- Observe et mène des études de prospection sur le risque numérique

POINTS PRINCIPAUX DES INTERVENTIONS ET ECHANGES

Intervention de Julien Chambon, maire de Houilles (78)

La commune de Houilles (78) a été victime d'une cyberattaque le 30 janvier 2021 en raison d'un logiciel malveillant qui s'est infiltré dans nos ordinateurs pendant le week-end. Nos données ont été cryptées ne permettant plus d'y accéder. Nous avons subi une incapacité totale à travailler. L'outil informatique a aujourd'hui une place prépondérante pour l'ensemble des agents et dans notre travail.

La commune avait déjà commencé à externaliser une partie de ses données, ce qui a permis d'être plus réactif face à l'attaque. L'enjeu majeur dans ce cadre était d'arriver à maintenir la continuité des services publics malgré la perte des outils de travail.

Quand l'attaque est massive, le numérique s'efface au profit du physique qui redevient systématique. Il y a un véritable besoin de personnels pour se rendre en local sur chaque poste de travail pour l'adapter, en temps de crise, à cette nécessité de continuité du service public.

Le plus dur est de réussir à trouver rapidement des professionnels qualifiés pour faire un diagnostic de l'attaque afin de travailler à la reconquête des données. La commune a dû embaucher quatre personnes à temps plein pendant plusieurs semaines pour ressaisir toutes les données et revenir à une situation normale. Il insiste sur la réactivité des TPE-PME sollicitées par la Mairie, bien plus humaines et mobilisables que les grandes entreprises.

Il faut absolument que les collectivités agissent, en amont, pour se prémunir de ces attaques.

Il y a un vrai intérêt d'investir sur le risque informatique et de mettre des moyens pour éviter l'impact fonctionnel et budgétaire sur la commune (environ 600 000€ de dépenses en raison de cette cyberattaque pour la commune de Houilles).

Intervention de Guillaume Crépin pour l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a été créée en 2009. Elle est rattachée au Premier ministre et au Secrétariat général de la Défense et de la Sécurité nationale (SGDSN). L'agence intervient uniquement sur le plan défensif et non offensif, qui est réservé au ministère des Armées.

L'ANSSI a trois grandes missions :

- La prévention et la sensibilisation de tous aux risques cyber : pour élever globalement le niveau de cyber sécurité
- La détection des incidents cyber : installation de « sondes » pour regarder ce qui se passe sur les réseaux et pour anticiper les attaques
- La réponse aux incidents cyber : des équipes opérationnelles disponible sur tout le territoire pour aider les services de l'Etat pouvant être paralysés

Ce qu'ils définissent comme système d'information : c'est l'ensemble des moyens informatiques et humains organisés pour collecter, stocker, traiter et communiquer des informations. La sécurité numérique consiste, elle, à assurer la sécurité de l'ensemble de ces biens de manière globale et cohérente. Il s'agit donc d'un vrai système en réseau.

Les actions de défense de l'ANSSI : sur le principe de la stratégie militaire de Vauban, l'agence multiplie des solutions de sécurité pour ralentir l'attaquant et épuiser ses ressources. Autrement dit, il y a une superposition de solutions techniques pour répondre aux attaques, avec notamment :

- La sensibilisation régulière des utilisateurs aux menaces et aux modes opératoires du moment
- Le renforcement des procédures en interne et avec les partenaires des organisations potentiellement ciblées

Le slogan « Tous connectés, tous concernés, tous responsables » rappelle la prédominance des actions de sensibilisation de tous les acteurs : agents, salariés, clients, fournisseurs, et sous-traitants.

Pour se tenir informé des bonnes pratiques et des menaces, l'ANSSI publie sur son site plusieurs guides, notamment à destination des collectivités territoriales et des décideurs publics.[3]

L'agence recense trois grands types de menaces numériques pouvant impacter les collectivités :

- La cybercriminalité : qui consiste essentiellement à extorquer de l'argent
- L'espionnage sur les systèmes d'information : qui consiste en des tentatives de piratages de données pour récupérer des secrets d'État, d'entreprise ou autres données sensibles
- Pré-positionnement dans les infrastructures : les malfaiteurs s'installent dans les systèmes d'informations en déployant des outils qui contaminent l'ensemble des machines. L'attaquant attend ensuite le moment opportun pour neutraliser tous les équipements.

[3] A retrouver sur le site de l'ANSSI, consultable à l'adresse suivante : Bonnes pratiques | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Qui sont les pirates informatiques ? Les attaquants ont différentes origines : il peut s'agir d'un Etat étranger, de leurs unités spéciales, de bandes criminelles organisées ou encore d'hacktivistes.

Focus sur les menaces pesant sur les élections de 2022 : Il y a un risque d'attaques cette année et de déstabilisation politique au profit d'intérêts étatiques étrangers visant à influencer le résultat de l'élection, à perturber le scrutin ou à nuire à l'intégrité du processus électoral. Concrètement, les pirates souhaitent agir pour perturber le décompte des voix, émettre des doutes sur l'intégrité des résultats et espionner les candidats.

Pourquoi les attaques numériques réussissent-elles si souvent ?

- **Un environnement favorable :** du fait de la numérisation croissante des outils numériques, de l'interconnexion numérique des acteurs, de la dématérialisation des données et de la complexité croissante des systèmes
- **Un avantage laissé à l'attaquant :** ces groupes organisés et spécialisés exploitent en toute discrétion les vulnérabilités des systèmes. N'étant pas découverts, ils peuvent prendre le temps de passer outre les systèmes primaires de défense

Quel rôle pour les élus ?

D'abord, impulser l'effort collectif : c'est-à-dire prendre conscience du risque pour impulser une dynamique générale de la collectivité en formant les parties prenantes à la cyber sécurité.

Ensuite, réévaluer le risque pour sa collectivité : le risque numérique n'est plus seulement un risque technique, il est pluridisciplinaire. Ce n'est plus un domaine à faire porter seulement par les techniciens de l'informatique.

Il est nécessaire de réévaluer complètement ses risques numériques, au même titre que les risques juridiques, financiers, sociaux ou environnementaux. **Agir pour une sécurité numérique est une décision qui doit être portée politiquement par les élus.**

L'ANSSI a édité un guide qui référence l'essentiel de la réglementation qui s'impose aux collectivités territoriales et propose des recommandations concrètes[4].

Le message à retenir, c'est qu'il faut se préparer à la crise car les attaques sont permanentes : **la question n'est plus de savoir si cela va arriver mais quand l'attaque réussira**. La gestion de crise numérique appelle une réponse d'ordre stratégique par les élus.

[4] Pour retrouver le guide, consultable à l'adresse suivante : Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Le conseil de l'ANSSI : « préparez-vous et exercez-vous ». C'est-à-dire de ne pas hésiter à mettre en œuvre dans les collectivités des exercices de crise face à une attaque numérique :

- Mettre en œuvre une pré-communication de crise après une attaque
- Préparer un plan global de gestion de crise après une attaque

Intervention de Laurent Verdier pour le Groupement d'Intérêt Public d'Action contre la Cyber malveillance (GIP ACYMA)

Cybermalveillance.gouv.fr est un dispositif national de sensibilisation, de prévention et d'assistance aux victimes qui a été lancé officiellement en 2017. La structure est créée de par la volonté de disposer nationalement d'un guichet unique apte à recueillir tous les publics victimes d'attaques numériques.

Les missions du dispositif Cybermalveillance.gouv.fr :

- Assister les victimes d'actes de cyber malveillances, informer et sensibiliser à la sécurité numérique, observer et anticiper le risque numérique
- Acculturer les particuliers, les entreprises et les collectivités territoriales aux cyber-attaques dans un langage non technique et accessible à tout le monde

Quelques données sur le Groupement d'Intérêt Public d'Action contre la Cyber malveillance (GIP ACYMA) :

- Son financement émane de 53 organisations publiques et privées
- La structure référence 1250 prestataires qualifiés sur l'ensemble du territoire
- Le GIP ACYMA a assisté, depuis 2017, 420 000 victimes d'attaques
- La structure a identifié et traité 48 types d'incidents numériques

Concernant les victimes, une plateforme numérique permet de diagnostiquer, de conseiller et de signaler ces attaques[5].

Le GIP ACYMA met concrètement en relation les victimes avec des prestataires qualifiés et ayant signés une charte d'engagement. Les détails de cette charte sont disponibles en ligne et en libre accès.[6]

[5] Consultable à l'adresse suivante : Outils de diagnostic - Assistance aux victimes de cybermalveillance
[6] Consultable à l'adresse suivante : chartev2.5.pdf (cybermalveillance.gouv.fr)

Les Principales causes de recherche d'assistance en 2020 pour les entreprises et les collectivités :

- Les rançongiciels
- Le piratage informatique
- Le piratage de compte
- L'hameçonnage

Les rançongiciels sont la 1ère menace pour les professionnels. Ces rançongiciels visent tous types et tailles d'organisations. Les méthodes employées sont celles du vol de données puis du chantage aux structures (demande de rançon pour récupérer les données).

Très important : il ne faut jamais accepter de payer une rançon !

L'ANSSI, le GIP ACYMA et la Banque des Territoires ont travaillé ensemble pour sensibiliser les élus aux risques numériques et pour partager avec eux les bonnes pratiques[7]. Trois volets de ce guide sont à retenir :

Volet 1 : les principales menaces et les réflexes essentiels en cas d'attaque

Volet 2 : vigilance toutes les collectivités sont concernés via les témoignages anonymes

Volet 3 : témoignages de collectivités ayant mise en place des actions de sensibilisation

Un questionnaire d'autoévaluation du risque numérique des collectivités : porté conjointement par l'AMF et la Gendarmerie Nationale en septembre 2020. Cet outil vise à aider les élus à évaluer leurs faiblesses potentielles de leurs infrastructures numériques.

Il n'y a pas un seuil de mauvaises réponses à partir duquel il faut s'inquiéter. Néanmoins, lorsque plusieurs réponses négatives sont cochées, il est fortement recommandé d'agir en sollicitant une expertise numérique pour sa collectivité[8].

La mise en œuvre d'un référentiel technique Expert Cyber : l'objectif est de reconnaître l'expertise en sécurité numérique, sur les activités d'installation, la maintenance et l'assistance, pour des clients aux besoins spécifiques (TPE-PME, associations, collectivités)

[7] Consultable à l'adresse suivante : Guide-collectivite-confiance-numerique.pdf (cybermalveillance.gouv.fr)

[8] Consultable à l'adresse suivante : 2021-124 Diagnostic Cyber V2.indd (amf.asso.fr)

Aujourd'hui, 171 organisations sont labélisées Expert Cyber sur l'ensemble du territoire.

Quelques gestes essentiels à retenir enfin pour la sécurité numérique des collectivités :

- Utiliser des mots de passe uniques et solides +activer double authentification
- Appliquer les mises à jour de sécurité
- Utiliser un antivirus
- Faire régulièrement des sauvegardes de vos données
- Rester vigilants !

Intervention de David Prache, start-up OPPENS

David Prache intervient pour aborder le facteur humain et les actions de formation à mener dans le cadre de la sécurité numérique des collectivités territoriales. Oppens est une filiale de la Société Générale. Elle est composée d'experts en cybersécurité. Elle agit pour protéger les entreprises, les associations et les collectivités.

La filiale dispose d'une habilitation « France Relance », mais n'est pas labelisée « Expert Cyber ». En effet, Oppens intervient surtout dans la formation et la sensibilisation des équipes.

Comment sensibiliser ses équipes ?

Outils phishU : beaucoup utilisé dans les entreprises, peu encore dans les collectivités. Cet outil permet de faire des « test de phishing », c'est-à-dire de simuler une attaque numérique pour mesurer le risque humain et vérifier la vigilance des collaborateurs.

Entrainement continu du fishing : il s'agit de séances de micro-learning (micro formation en ligne de quelques minutes) pour former les agents en continu avec des exercices de phishing répétés quatre fois par an.

Ces entraînements permettent de mesurer la progression des collaborateurs au fil des trimestres. La répétition des sensibilisations est primordiale pour lutter contre la courbe de l'oubli.

Les formations : en présentiel ou à distance sur les différentes thématiques du cyber sur des formats de vingt minutes pour comprendre comment fonctionnent, concrètement, les pirates informatiques.

Les prestations de protection pour les collectivités avec les partenaires de la filiale OPPENS :

- La réalisation de tests d'intrusion dans le système informatique
- La mise à disposition de coffres-forts électroniques pour les données

- Des solutions assurantielles contre les attaques numériques
- Des actions de sensibilisation du personnel et des agents

Ces prestations viennent en complément de l'ANSSI et de Cyber malveillance et ne sauraient remplacer l'expertise qu'ils mettent en œuvre.

Questions des participants

Est-ce que la mairie a mis en place un budget dédié à la cybersécurité à la suite de l'attaque ?

Julien Chambon précise qu'un pare-feu leur a coûté entre 15 000 et 20 000 euros. Avec le déploiement d'un antivirus proactif, les coûts sont évalués à environ 90 000 euros pour un parcours complet de cyber sécurité. Des demandes de subventions ont aussi pu être faites.

La mairie de Houille était-elle assurée à ce moment avec une intervention correcte ou non ?

Julien Chambon précise que la commune était assurée mais qu'ils n'ont obtenu que 5 000€ de l'assurance.

Avez-vous réfléchi à un changement d'assurance ? Retour d'expérience sur qualité d'expérience ?

Julien Chambon propose aux élus de le recontacter pour que ses services fassent un communiqué à ce propos.

Comment trouver une assurance à des tarifs accessibles et suffisamment efficace ?

L'assurance doit faire partie d'un package intégrant les risques juridiques et la couverture assurantielle.

Quelles sont les impacts en matière de « stress » sur les agents et les habitants ?

Julien Chambon explique qu'il y a eu une réaction assez solidaire avec des ressources trouvées au sein des services embarqués dans le dispositif d'urgence et de crise, suscitant moins d'angoisse et moins de stress.

Quel est votre avis sur le fait de rendre illégal le paiement de rançon ?

Guillaume Crépin précise qu'il ne faut surtout pas payer la rançon car vous alimentez un système, vous n'êtes pas certain de récupérer vos données ni dans un format lisible. Il faut aussi souvent payer pour récupérer l'usage de l'ensemble de la bureautique.

Si vous payez la rançon, c'est une somme que vous n'utiliserez pas dans la reconstruction du système d'informations.

Si on interdit le paiement des rançons, cela n'empêche pas les attaques de se mener car elles sont internationales. Le modèle économique de cyber-attaques repose sur la détresse de la victime, **il faut plutôt travailler de manière pédagogique en faisant comprendre à la victime que le paiement de la rançon reste un système crapuleux dans lequel il n'y a aucune garantie.**

LISTE DES INSCRITS

NOM	PRENOM	COMMUNE	FONCTION
CZEPCZAK	RAPHAEL	CERNAY LA VILLE 78720	Maire Adjoint Développement Durable
MESA	STEPHANE	ROSNY-SOUS-BOIS	Rattaché(E) A Un Service D'une Collectivité - Chef De Cabinet
CATINAUD	ALAIN	SUCY-EN-BRIE	Conseiller Municipal En Charge Du Numérique
AIT	EDDIE	CARRIERES SOUS POISSY	Maire
MARLIER	SANDRINE	COUBRON (93)	Rattaché(E) A Un Service D'une Collectivité - Secrétaire Cabinet Du Maire
BELLINELLI	GUILLAUME	MAIRIE DE ROINVILLE	Maire De ROINVILLE
CHALANE	HAKIM	AMIF PARTENAIRES	Consultant Senior - Gestions Locales Formation Conseil Aux Collectivités Territoriales
BELLINELLI	GUILLAUME	MAIRIE DE ROINVILLE	Maire
LAMBILLIOTTE	FLORIANDRE	JOINVILLE-LE-PONT 94340	Rattaché(E) A Un Service D'une Collectivité - Chef De Cabinet
EL HAÏTE	NAJWA	ÉVRY-COURCOURONNES	Adjointe Au Maire
ORZECH	DAVID	ORANGE	AMIF Partenaires - Directeur Des Relations Avec Les Collectivités Locales Du Val De Marne
LEDEUR	DIDIER	95120 ERMONT	Adjoint Au Maire
BELLINELLI	GUILLAUME	MAIRIE DE ROINVILLE	Maire
JEBARI	SORAYA	ROMAINVILLE 93230	Conseillère Municipale
COQUELET	CHRISTIAN	FAVIERES 77220	Conseiller Municipal Délégué Au Numérique Et A L'urbanisme
NGO	QUYNH	MAIRIE DE MORANGIS (91420)	Adjointe Au Maire
GIRAUD	PIERRE	75015	AMIF Partenaires - Responsable Technique
WIOLAND	HERVE	BUC - 78530	CM Délégué A La Sécurité
NICOLAS	CEDRIC	92340 - BOURG-LA-REINE	Maire Adjoint Délégué Aux Mobilités Et Au Numérique
BLIVET	JEAN-PHILIPPE	VILLEPREUX	Conseiller Delegue A La Securite Publique Et Operationnelle
CHARLES	NORMAN	VIGNEUX SUR SEINE 91270	Adjoint Au Maire
SLOWIK	BRUNO	FEUCHEROLLES 78810	Responsable Informatique

VALENTIN	JEAN-PIERRE	CARRIERES-SUR-SEINE	Adjoint Si
VANESON	JOCELYNE	COURTOMER 77390	Maire
REFALO	PAULINE	IGNY 91430	Directrice De Cabinet Et De La Communication
GUTIEREZ	GREGORY	MALAKOFF 92240	Conseiller Municipal Délégué "Numérique Et Citoyenneté"
GOMPERTZ	STEPHANE	78450 CHAVENAY	1er Adjoint
SALA	PATRICK	BUSSIERES 77750	Adjoint Au Maire
BOUQUIN	NADINE	VAUCRESSON 92420	Maire-Adjointe
AÏT	EDDIE	CARRIERES-SOUS-POISSY 78955	Maire
CHAIBELAINE	DALILA	RUNGIS 94150	Adjointe Au Maire A La Communication, Au Numérique, A La Ville Connectée
SONDEJ	FREDERIC	CARRIERES-SUR-SEINE - 78420	Dsi
LEHMANN	PHILIPPE	EGLY - 91520	1er Adjoint
COSTI	PIERRE	PALAISEAU	Adjoint Résilience Et Risques
FOURNIER	DOMINIQUE	MORMANT 77720	Conseiller Municipal
FLAMAND	JULIE	BREVAL 78980	Adjointe
LAFEUIL	CYRILL	SOUPPES-SUR-LOING 77460	Conseiller Municipal Délégué Au Numérique
COSTI	PIERRE	PALAISEAU	Adjoint Au Maire Résilience Et Gestion Des Crises
SARRAT	ERIC	VERNOUILLET 78540	Conseiller Municipal
SALA	PATRICK	BUSSIERES 77750	Adjoint Au Maire
BOUQUIN	NADINE	VAUCRESSON	Maire-Adjointe
AVOGNON	CLEMENCE	FONTENAY-SOUS-BOIS	Adjointe Au Maire
DESAMAISON	GUY	LESIGNY - 77150	Adjoint
MOUTENOT	LAURENT	CONFLANS-SAINTE-HONORINE - 78700	Adjoint Au Maire
LEFEVRE	THIERRY	ISSY LES MOULINEAUX 92130	Premier Maire-Adjoint
VERGERON	CHRISTOPHE	BOULOGNE – BILLANCOURT 92100	Directeur De Systèmes d'Information
TRIPOT	CHRISTIAN	OTHIS-77280	Maire-Adjoint Aux Finances Et Numérique
LEDEUR	DIDIER	ERMONT 95120	Adjoint Au Maire