PRÉFET
D'ILLE-
ET-VILAINE
Liberté
Égalité
Fraternité

SÉCURITÉ NUMÉRIQUE DÉPARTEMENTALE

Mars 2024

ÉDITORIAL DU PRÉFET D'ILLE-ET-VILAINE

Mesdames, Messieurs,

Si notre département était jusqu'à présent préservé des cyberattaques massives, 2023 a sonné le glas de cette période préservée. Nous assistons en effet à un véritable tournant dans les actions offensives visant nos institutions dans le cyberespace. Le CHU de Rennes et la ville de Betton ont ainsi été attaqués par des collectifs internationaux de cybercriminels.

Les impacts de telles attaques peuvent être majeurs à l'échelle d'une collectivité. Maillons essentiels de la relation entre l'État et les citoyens, les collectivités territoriales sont notamment dépositaires de données personnelles que nous devons protéger.

Dans le domaine informatique, le recours à l'externalisation est devenu une pratique courante qui présente un certain nombre d'avantages, mais aussi de risques qu'il convient d'évaluer. C'est pourquoi j'ai souhaité la mise en place d'un document facilitant la gestion et la compréhension des enjeux liés à l'infogérance afin de vous assister dans une démarche de prévention. Il est en effet apparu que ce type de guide n'existait pas. J'espère que cette innovation bretillienne vous sera pleinement utile.

Je tiens à remercier chaleureusement les organismes impliqués dans ce travail : l'AMF 35, l'AMR 35, la gendarmerie nationale, l'agence nationale de la sécurité des systèmes d'information, le centre de gestion de la fonction publique territoriale, Mégalis Bretagne et le centre de réponse aux incidents de sécurité numérique de la région Bretagne, «Breizh cyber», qui renforce depuis novembre 2023 notre résilience numérique départementale.

La lutte contre les menaces d'origine cyber ne peut être menée individuellement : la sécurité du numérique est l'affaire de tous !

Philippe Gustin,
Préfet d'Ille-et-Vilaine

L'ÉTAT DES LIEUX

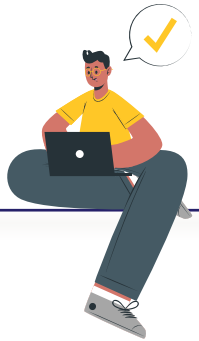
L'infogérance informatique consiste à sous-traiter à un prestataire externe la prise en charge de tout ou une partie des besoins informatiques d'une collectivité. Vous avez probablement recours à un ou des prestataires informatiques pour différentes raisons qu'il convient de se remémorer à travers un rapide état des lieux. Vous souvenez-vous de l'objectif de base ? Pourquoi avez-vous décidé de confier la gestion, l'exploitation ou l'optimisation de vos systèmes d'information à un prestataire extérieur ?

Pourquoi ai-je recours à l'externalisation ?

- La réduction des budgets alloués
- L'absence ou la perte des compétences nécessaires
- La simplicité de gestion
- La mise en conformité avec les exigences légales et réglementaires

Recourir à **l'externalisation n'est pas exempt de risques de sécurité.**

L'encadrement de vos relations contractuelles est essentiel pour vous prémunir des différents risques.



LES NOTIONS ESSENTIELLES

Externalisation informatique : En informatique, l'externalisation est une opération consistant à confier à un prestataire tiers, infogéreur, le soin d'exploiter, administrer, maintenir tout ou une partie seulement d'un système informatique.

Analyse de risques : Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

Exigences de sécurité informatique : Une exigence est un contrat entre un fournisseur et son client qui doit être décrite sous la forme d'une action. Elle précise ce que l'on veut faire. A ce titre, la collectivité territoriale doit s'assurer des exigences de sécurité en termes de disponibilité, d'intégrité, de confidentialité et traçabilité des données.

- *Exemple 1 : Vous êtes maire d'une commune, une personne a porté atteinte volontairement ou non à l'intégrité d'un document important. Cette modification illégitime doit pouvoir être détectée et corrigée.*
- *Exemple 2 : En informatique, la disponibilité a pour but de garantir l'accès à une application, un système, une donnée. Le logiciel de rançon (ou ransomware en anglais) a justement la particularité de porter atteinte à la disponibilité des données ou d'un système d'information en échange d'une rançon. Quelles sont les mesures mises en place par votre prestataire pour garantir cette exigence de disponibilité ?*

Plan d'assurance sécurité (PAS) : Le plan d'assurance sécurité est un document contractuel rédigé par le prestataire, il décrit les moyens que ce dernier met en œuvre pour répondre aux différentes exigences décrites dans le marché. C'est un cadre de réponse qui offre une structure pour la réponse des candidats aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite la comparaison entre les différentes offres. Une fois le prestataire retenu, le PAS est annexé au contrat.

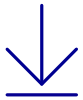
INCIDENT NUMÉRIQUE
LES RISQUES D'UNE MAUVAISE EXTERNALISATION

Des dépenses non budgétées (de quelques milliers à centaines de milliers d'euros)

Une perte de confiance des citoyens et une image négative de la collectivité, des élus, des agents.

Une responsabilité pénale en tant que responsable de traitement (selon le RGPD)

Des services à la population rendus inopérants



De potentielles destructions des données et perte du patrimoine informationnel.

Des conséquences pour les usagers : Usurpation d'identité, escroquerie, ouverture de compte, etc.

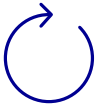
Les métiers de l'externalisation et de la cybersécurité sont des métiers différents

LES QUESTIONS À SE POSER

Êtes-vous en mesure de répondre aux questions suivantes concernant votre contrat avec votre prestataire ?

Où sont géographiquement situées les données que vous lui confiez ?

Comment puis-je exercer mon droit de regard et de contrôle sur les données ?



Est-ce que des sauvegardes existent et sont-elles testées régulièrement ?

Tous les composants de mon système d'information sont-ils bien couverts par un contrat ?

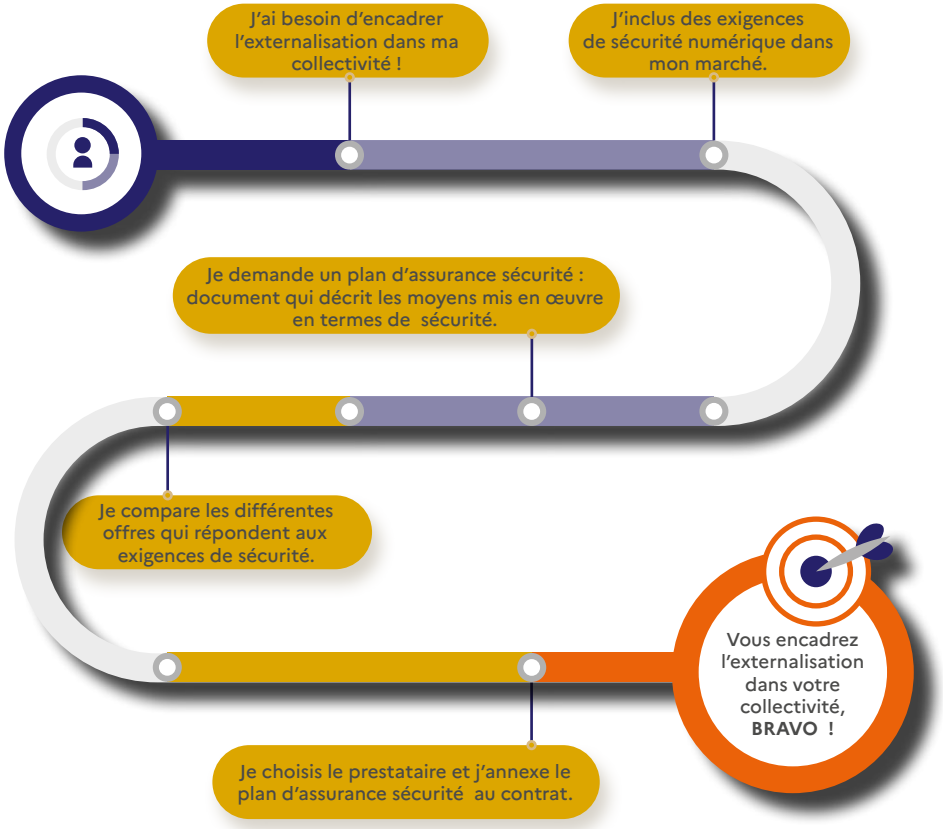
Des mises à jour régulières de vos systèmes d'information sont-elles effectuées et des rapports vous sont-ils communiqués ?

Comment votre prestataire gère-t-il la sécurité et la confidentialité des données que vous lui confiez ?

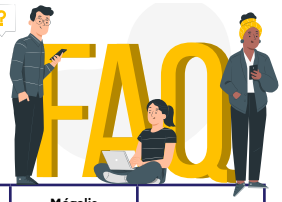
VOUS CONNAISSEZ VOTRE PRESTATAIRE DEPUIS DES ANNÉES ? ATTENTION DANGER !

Confiance et compétence sont deux notions différentes. **La confiance n'exclut pas le contrôle.** À défaut, vous pourriez être exposé à de sérieuses vulnérabilités. Question à vous poser : votre prestataire est-il monté en compétences ces dernières années : certifications, diplômes, formations ?

COMMENT AMÉLIORER MES CONTRATS ?



J'AI BESOIN D'AIDE, À QUI M'ADRESSER ?



Foire aux questions (FAQ)	ANSSI	GIP ACYMA*	Gendarmerie	AMRF35	AMF35	CDG35	Mégalis Bretagne	Préfecture
J'ai besoin d'informations complémentaires sur les risques liés aux prestations informatiques.	•					•		
Je souhaite bénéficier d'un premier diagnostic.			•			•	•	
Où-puis je trouver un modèle de plan d'assurance sécurité et les annexes ?	•				•	•	•	
J'ai des besoins en sensibilisation à la sécurité du numérique dans ma mairie/communauté de communes.			•			•	•	
J'ai besoin d'information/aide pour le plan communal de sauvegarde (PCS).				•	•			•
Quelle(s) ressource(s) grand public pour s'informer sur les menaces numériques ?	•	•	•					

**Groupement d'intérêt public « Action contre la Cybermalveillance »*

Le CDG35, Mégalis Bretagne et la Gendarmerie Nationale sont des acteurs à privilégier pour vous accompagner dans vos travaux de sécurisation.

POUR ALLER PLUS LOIN

Thématique	Lien vers la source
Toutes les actualités de l'ANSSI	https://cyber.gouv.fr/
Le guide d'hygiène informatique en 42 mesures (à fournir à votre prestataire informatique)	https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
Dispositif de formation à la sécurité du numérique	https://secnumacademie.gouv.fr/
Guide AMF/ANSSI	https://cyber.gouv.fr/publications/cybersecurite-toutes-les-communes-et-intercommunalites-sont-concernees
Label « Expertcyber »	https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/label-expertcyber
Visa de sécurité : «SecnumCloud»	https://cyber.gouv.fr/actualites/zoom-sur-secnumcloud-et-la-protection-des-donnees
Dossier «Conseils»	https://www.gendarmerie.interieur.gouv.fr/conseils

Les sociétés privées peuvent également vous accompagner dans vos démarches. Certaines entreprises de services informatiques justifiant d'une expertise en sécurité numérique et sont labellisées « ExpertCyber », label développé par *cybermalveillance.gouv.fr*. L'agence nationale de la sécurité des systèmes d'information (ANSSI) met à jour régulièrement une liste de prestataires de services de confiance que vous pouvez consulter.

Préfecture d'Ille-et-Vilaine

www.ille-et-vilaine.gouv.fr | @prefetbretagne | @bretagnegouv

Conception et réalisation : Préfecture d'Ille-et-Vilaine, février 2024 | Crédits illustration © storyset.