#CYBERFENUA2018

Cahier des charges de l'exercice « CYBERFENUA 2018 » pour préparer les entreprises et les communes polynésiennes à répondre à des attaques cybercriminelles

Table des matières

La Polynésie française souhaite organiser les 3 et 4 octobre 2018 une nouvelle édition de l'exercice CYBERFENUA, exercice qui vise à se préparer à répondre à toutes attaques cybercriminelles.

Pour CYBERFENUA 2018, la Polynésie française souhaite externaliser les prestations de gestion logistique et organisationnelle de l'exercice.

1. L'objectif de l'exercice « CYBERFENUA 2018 »

L'exercice « CYBERFENUA 2018 » vise à définir et valider les mesures à mettre en œuvre en cas de cyber-attaque massive visant les communes, les TPE/PME et les particuliers sur le territoire de la Polynésie française.

L'exercice de simulation « CYBERFENUA 2018 » a vocation à tester les capacités des acteurs publics, privés, communaux et associatifs, à faire face à des situations et attaques informatiques d'envergures sur des équipements informatiques, de télécommunications, notamment par le biais de programmes malveillants.

L'objectif de cette édition doit permettre aux :

- acteurs associatifs d'être les vecteurs de transport de l'information auprès des entreprises du secteur ;
- communes de se prémunir notamment en adaptant les techniques de protection les plus modernes en matière de cyber-protection.

« CYBERFENUA 2018 » doit également permettre la préparation de tous les acteurs à combattre la cybercriminalité notamment en coordination avec l'Agence nationale de sécurité des systèmes d'informations.

2. Le concept de l'exercice « CYBERFENUA 2018 »

CYBERFENUA 2018 s'appuie sur plusieurs points :

1- Les acteurs impliqués :

- Le gouvernement et l'administration de la Polynésie française,
- Les communes : 3 communes cibles, le SPC-PF et le CGF,
- Les entreprises du secteur des télécommunications,
- Les TPE, les PME ainsi que les associations patronales et professionnelles regroupant des experts de la sécurité informatique et du numérique,
- Une « *Task force citoyenne* » composée d'étudiants, chargée d'intervenir auprès des particuliers et des TPE afin de procéder aux opérations de remise en route des systèmes informatiques touchés.

2- La sensibilisation des acteurs :

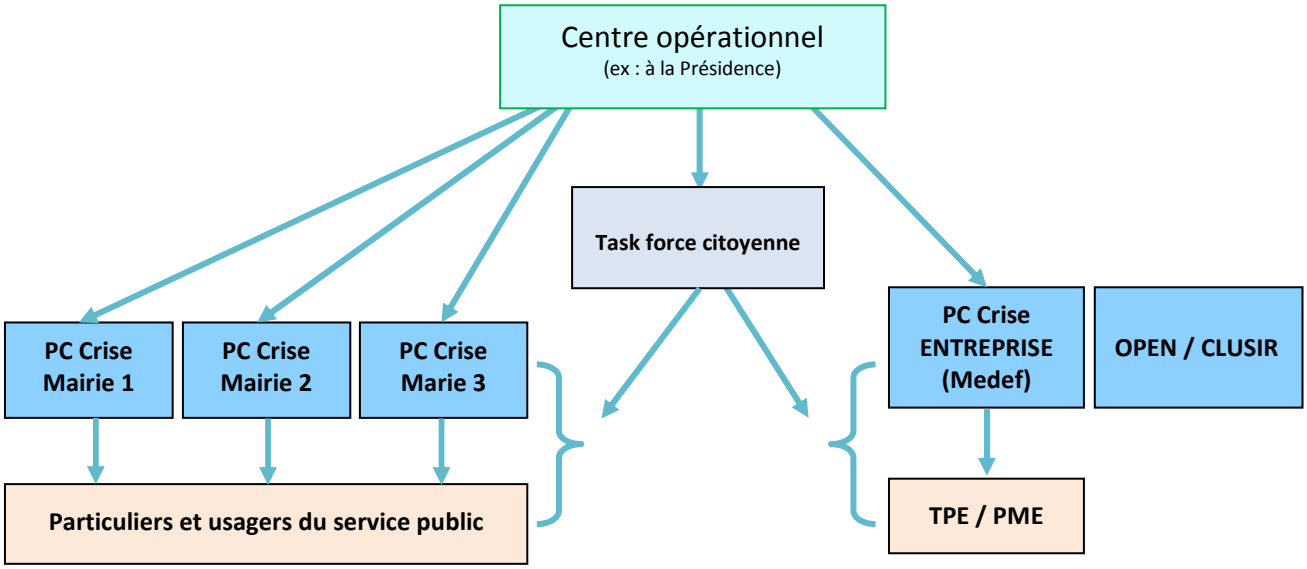
- Il s'agit de s'assurer que les acteurs impliqués disposent en préalable des outils nécessaires à la mise en œuvre d'un centre opérationnel, à la gestion de crise et à la conduite d'opérations ;

3- La mise en œuvre de postes de commandement de crise :

- Le poste de commandement (PC) est en charge des phases de réflexion, de conception et de conduite des opérations. L'impact sur le terrain se veut être limité, seules quelques

phases pourraient être simulées (dans le cadre de l'exercice, la diffusion d'ordre vaudra exécution des tâches) ;

- Les différents niveaux « hiérarchiques » : gouvernement et communes ;
- Les différentes localisations (Présidence et mairies impliquées) ;
- La coordination Public et Privé : intégration d'une composante « entreprise » qui pourrait être coordonnée par le MEDEF.



4- *L'organisation de l'exercice :*

- Durée : L'exercice se déroulera sur 2 jours ;
- Modalité : l'exercice se jouera en temps accéléré (x4 maximum) afin de permettre à chaque niveau de PC de prendre part au rôle qui lui incombe ;

5- *Le déroulement de l'exercice :*

- Une phase préliminaire de mise en alerte et de montée en puissance des PC. Cette phase préliminaire devra être jouée en temps réel afin d'évaluer les chaînes d'alerte et les procédures logistiques de mise en œuvre d'une cellule de crise et d'un PC ;
- Une phase de retour à la normale simulée en partie sur le terrain avec la coordination et le déploiement de la « *Task force citoyenne* » en vue de remettre en service les systèmes informatiques et de télécommunications affectant les usagers des services ;

3. Le scénario de l'exercice « CYBERFENUA 2018 »

Afin d'évaluer les capacités d'adaptation des acteurs impliqués en cours d'exercice, le scénario comportera 2 phases :

1. Une première phase de réponse à des intempéries exceptionnelles (fortes pluies), localisées sur Tahiti mais dont l'impact en matière de sécurité civile restera limité aux compétences, interventions et prises de décisions de la Polynésie française. À ce titre, cette phase ne devra en aucun cas concevoir de risques pour les personnes physiques ou les populations ;

2. Une seconde phase pendant laquelle des hackers profiteront d'une situation déjà tendue pour lancer une attaque de type « zero-day » non ciblée. Cette attaque touchera les systèmes informatiques et de communications les moins bien protégés, notamment ceux des communes, des TPE/PME et des particuliers.

Le prestataire retenu proposera un scénario détaillé, au plus tard 8 semaines après sa notification, et sa mise en œuvre déclinée dans le cadre de l'exercice.

4. **Le périmètre des prestations attendues**

Le prestataire assure en lien avec la Polynésie française :

1. La détermination et l'animation du programme de préparation préalable des acteurs à l'exercice ;
2. La mise en œuvre des chaînes d'alerte des structures de crise impliquées ;
3. La mise en alerte d'une chaine spécifique CYBER ;
4. La mise sur pied des PC crise ;
5. L'activation des PC crise des communes retenues ;
6. Le test des liaisons entre les PC crise de différents niveaux ;
7. La mise en place des procédures de circulation de l'information entre les PC ;
8. La mise sur pied de la « Task force citoyenne » ;
9. La mise en place d'un média-center pour gérer la relation presse (communication de crise).

Le prestataire retenu, devra disposer d'une expérience reconnue et avérée en matière de gestion logistique, animation d'atelier et d'organisation de formation en gestion de crise.
Par ailleurs, une bonne appréhension du paysage digital polynésien et une expérience avérée sur des exercices locaux ou nationaux seront un atout important.

La présente consultation se compose d'un lot unique comportant :

1. La phase de préparation préalable du **Centre opérationnel (CO) et des entreprises (PP1),**

   Les objectifs pédagogiques de cette phase de préparation préalable des acteurs à l'exercice PP1 sont les suivants :
   - Connaître les principes fondamentaux de gestion de crise,
   - Connaître la composition et les procédures d'un centre opérationnel,
   - Mettre en œuvre les moyens d'un centre opérationnel,
   - Élaborer une stratégie de communication de crise tous médias.

   Nombre de personnes : 30 maximum

2. La phase de préparation préalable des **acteurs communaux (PP2),**

   Les objectifs pédagogiques de la phase de préparation préalable des acteurs à l'exercice PP2 sont les suivants :
   - Connaître les principes fondamentaux de gestion de crise ;
   - Connaître son PCS ;
   - Activer et mettre en œuvre le PCS ;
   - Informer, la population et les usagers.

   Nombre de personnes : 20 maximum

Les deux phases de préparation préalable des acteurs (CO, PP1 et PP2) à l'exercice, devront se dérouler au moins 15 jours avant la tenue de l'exercice « CYBERFENUA 2018 », et le contenu pédagogique devra être soumis et validé par la DGEN.

3. **La proposition d'un scénario** complet et détaillé de l'exercice,

4. Les **prestations logistiques** liées à l'organisation de l'exercice « CYBERFENUA 2018 », sont les suivantes :

    - Coordination de la mise à en place du matériel sur chaque PCS ;
    - Gestion des matériels, des locaux et moyens généraux mis à disposition ;
    - Aide à l'installation et désinstallation des PCS ;
    - Gestion de l'accueil
    - Fourniture de repas légers et de boissons pour le Centre opérationnel et le PC Crise Entreprise ;
    - Conception d'un Kit Pratique regroupant toutes les informations utiles à l'exercice ;
    - Conception du dossier de presse ;
    - Conception de 2 roll-ups de signalement de l'exercice ;
    - Gestion des relations médias locaux : invitation aux conférences de presse, promotion de l'événement et auprès des rédactions pour calage interviews, plateaux et émissions TV et Radio avant et pendant l'événement ;

    Nombre de personnes : 70 maximum

5. L'**animation de l'exercice**, par la mise à disposition d'un référent disposant d'une expérience sérieuse en gestion de risque informatique et télécommunications.

Le prestataire retenu s'engage à travailler de la façon la plus transparente et la plus collaborative possible avec la Direction générale de l'économie numérique-DGEN, le ministère en charge du numérique et l'ensemble des acteurs associés à la phase de préparation de l'opération.

5. Les principes de la consultation

a. Planning de consultation et de production

Envoi de la consultation :	31/05/18
Réponses attendues par les soumissionnaires :	**02/07/18 avant 10h**
Fin de l'analyse et sélection :	06/07/18
Annonce du prestataire retenu :	09/07/18 à 10h

b. Contenu

La proposition devra comprendre a minima les éléments suivants :

- Démarche méthodologique proposée ;
- Calendrier faisant apparaître les étapes de la prestation ;
- Équipe et partenaire(s) retenu(s) pour la prestation ;
- Montant détaillé de la prestation ;
- Références significatives en matière de gestion d'évènementiel et gestion de crise.

c. *Format*

La proposition commerciale doit être limitée à 20 pages (annexes comprises) et sera réalisée en langue française, de préférence au format Word.

d. *Interlocuteurs*

Les propositions devront être envoyées simultanément aux adresses emails suivantes :

1. karl.tefaatau@dgen.gov.pf
2. manava.laborde@dgen.gov.pf

L'analyse des offres des prestataires sera réalisée par la Direction générale de l'économie numérique :

1. Monsieur Karl TEFAATAU ;
2. Madame Manava LABORDE ;
3. Monsieur Cyriaque MAIRE.

e. *Fractionnement de la prestation et territorialité*

Les prestations à conclure sont des prestations par convention avec un seul opérateur économique.
Le prestataire retenu pourra sous-traiter à un tiers, tout ou partie de ses droits et obligations issus de la prestation.
Le cas échéant il en informera la DGEN et Ministre en charge du numérique. Ce dernier pourra formuler un refus formel.
Peuvent répondre à la présente consultation les sociétés disposant d'un numéro TAHITI et à jour de leurs obligations fiscales.

f. *Plafond budgétaire alloué à l'exercice « CYBERFENUA 2018 »*

Le plafond maximum du budget alloué à la mise en place de l'exercice « CYBERFENUA 2018 » est de ***cinq millions de francs CFP (5 000 000 F CFP) toutes taxes comprises***.

Toutes négociations ou pénalités qui pourront être effectuées seront conformes aux dispositions du code polynésien des marchés publics.

g. *Modalités et conditions d'éligibilité des candidats*

Pour être éligible, les candidats devront fournir les pièces administratives suivantes :

- ☐ Extrait du registre du commerce (Kbis) de moins de 3 mois ;
- ☐ Situation au répertoire des entreprises via ISPF - N° Tahiti ;

- ☐ Relevé d'identité bancaire au nom du porteur de projet (RIB) ;
- ☐ Attestation de régularité en matière d'impôts directs territoriaux, délivrée par la Direction générale des finances publiques (Paierie de la Polynésie française), au nom de l'entreprise ;
- ☐ Attestation délivrée par la Caisse de prévoyance sociale – CPS, indiquant que l'entreprise est en situation régulière au regard de ses obligations sociales ;
- ☐ Attestation délivrée par la Direction des impôts et des contributions publiques que l'entreprise est en situation régulière au regard de ses obligations fiscales ;
- ☐ CV des membres de l'équipe.

6. **Les critères d'analyse des offres et les pondérations associées**

1. Qualité et détail de la proposition commerciale	5/100
2. Capacité à répondre au périmètre de la prestation	30/100
3. Montant de la prestation	30/100
4. Expertise de l'équipe proposée	10/100
5. Références de la société en matière de gestion de risque	25/100