Pū Ti'aauraae Faaineineraa Tōro'a

République française
Polynésie française

CONCOURS DE RECRUTEMENT DE LA FONCTION PUBLIQUE COMMUNALE AU TITRE DE L'ANNÉE 2022

ÉPREUVE D'ADMISSIBILITÉ N°2 : NOTE ADMINISTRATIVE

SPÉCIALITÉ TECHNIQUE SYSTEMES D'INFORMATIONS
CADRE D'EMPLOIS : CONCEPTION ET ENCADREMENT » (CATEGORIE A)
GRADE : CONSEILLER

Durée : 4 h

Coefficient : 3

⚠ À lire attentivement avant de traiter le sujet ⚠

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre prénom, ni votre nom ou nom fictif, ni signature, ni initiale ou paraphe.
- Seul l'usage d'un stylo noir ou bleu est autorisé. L'utilisation d'une autre couleur, pour écrire ou souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- Les feuilles de brouillons ne seront pas prises en compte.
- Les feuilles de suite seront agrafées à votre feuille de composition par le surveillant chargé de relever votre copie.
- Tous les candidats doivent remettre une copie, même blanche. Dans cette hypothèse, ils signent leur copie en indiquant « copie blanche ».

Ce document de 28 pages comprend un sujet de 3 pages et un dossier de 25 pages.
S'il est incomplet, en avertir un surveillant.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble Ia ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Pū Ti'aauraae Faaineineraa Tōro'a

République française
Polynésie française

CONCOURS POUR LE RECRUTEMENT DE CONSEILLER (catégorie A)

Spécialité technique
Systèmes d'informations

SESSION 2022

Note administrative rédigée à partir d'un dossier portant sur la spécialité ayant pour objet de vérifier les capacités à piloter des projets publics et les capacités rédactionnelles, afin de dégager des solutions opérationnelles appropriées. Cette épreuve fait appel à l'esprit d'analyse et de synthèse ainsi qu'à l'aptitude à situer le sujet traité dans son contexte général.

Durée : 4 h
Coefficient : 3

SUJET : La protection du système d'information de votre mairie

Vous êtes le responsable informatique de la commune X située en Polynésie française.

Dans un contexte international et national particulièrement sensible, votre mairie est la cible depuis quelques jours d'une campagne de diffusion de courriels frauduleux.

Contrairement aux attaques précédentes, les expéditeurs sont vos correspondants habituels et les sujets en rapport avec ceux que vous traitez habituellement.

La précision et la véracité de ces envois augmentent de manière considérable le niveau de risque et fragilisent votre système d'information.

La DGS craint une attaque qui cible l'intégrité du système d'information dans sa globalité et demande que vous rédigiez une note à son attention pour lui exposer :

1. Les mesures de protection actuellement en place qui protègent le système d'information et son évolution nécessaire à court terme.

2. Les pistes d'amélioration que vous proposez de mettre en œuvre à moyen et long terme.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

DOCUMENTS JOINTS

Document 1 : Élément de contexte. 1 page (F. POLLET, 4 juin 2022) ;

Document 2 : Le piratage de compte, fiche pratique. 2 pages (Publié sur www.cybermalveillance.gouv.fr, consulté en juin 2022) ;

Document 3 : L'importance de réaliser un audit en entreprise, extrait de la page d'accueil du site internet de « SYS UP ». 2 pages (Publié le 16 février 2021 sur www.systup.com) ;

Document 4 : Les collectivités face aux enjeux de cybersécurité, extrait d'infographie. 7 pages (Agence nationale de la sécurité des systèmes d'information, version 01 d'avril 2021) ;

Document 5 : Piratage informatique : une formation pour sensibiliser les cadres communaux, extrait d'un article de « Tahiti infos ». 2 pages (Publié le 08/03/2016) ;

Document 6 : Les 10 astuces pour sécuriser votre poste de travail en moins de 5 minutes, article internet. 3 pages (Lydie BALFET, publié le mardi 08 mars 2016 sur www.gpomag.fr/web/technologies) ;

Document 7 : Cyberattaques : quand les collectivités cherchent la parade, extrait d'article internet. 5 pages. (Stéphane PREVOST publié le 07/03/2022, modifié le 12/05/2022, https://www.stromshield.com/fr/actus/cyberattaques-quand-les-collectivités-cherchent-la-parade)

Document 8 : 9 conseils pour maintenir un SI robuste et sécurisé, document composé. 3 pages (F. POLLET d'après une infographie et les articles publiés sur https://www.alcees.com, consultés le 16 juin 2022).

Certains documents peuvent comporter des renvois à des notes et à des documents non fournis car non-indispensables à la compréhension du sujet.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 1 : Élément de contexte

1) Parc informatique

70 PC fixes dont 50 % du parc a plus de 5 ans.

20 PC portables dont 50 % des machines ont plus de 5 ans.

2 stations blanches sous SOFOS (Linux) avec mise à jour automatique via internet.

Les ports USB sont verrouillés et le parc-feu activé par défaut.

2) Serveurs

Un serveur Contrôleur de domaine sous windows 2012R2 renouvelé en 2016

Un serveur de fichier windows 2012R2 renouvelé en 2016

Un serveur d'impression renouvelé en 2016 virtualisé (VM Ware)

Un serveur Web internet virtualisé renouvelé en 2016

3) Logiciels

Windows 10 Entreprise version 20H2 sur l'ensemble du parc fixe/mobiles

Suite office 365 Pro, Pack MsOffice 2013, Antivirus Norton sur chaque machine

Quelques applications métiers développées localement en Java et en PHP.

Firefox est le navigateur par défaut.

4) Réseau Local (LAN)

Réseau local à plat non segmenté logiquement (VLAN)

Tous les ports sont en mode Access, dans le Vlan par défaut

5) Internet

Un réseau Wifi ouvert qui assure la totalité de la couverture du site connecté à une ViniBox Pro 30Mb/s de débit

6) Multimédia

Une salle de réunion équipée d'un téléviseur grand écran connecté qui permet la réalisation de toutes les Web conférences (Teams, Zoom…) au travers du réseau Wifi.

7) Téléphonie fixe

Téléphonie sur IP Alcatel

8) Compétences

Le technicien système qui a déployé les architectures virtualisées fait valoir ses droits à la retraite.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 2 : Le piratage de compte

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LE PIRATAGE DE COMPTE

COMPRENDRE LES RISQUES

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne. En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières : le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (***phishing*** en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

BUT RECHERCHÉ

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).

SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS.** Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez-en un solide (voir notre fiche sur la gestion des mots de passe). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION.**

CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Utilisez des mots de passes différents et complexes pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

Lorsque le site ou le service le permettent, **activez la double authentification** pour augmenter le niveau de sécurité.

Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Maintenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide.

Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer d'éventuelles connexions anormales.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate.

Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal)** : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

Dans le cas d'un piratage d'un compte de messagerie :
- **Atteinte au secret des correspondances (article 226-15 du code pénal)** : délit passible d'une peine d'emprisonnement d'un an et de 45 000 euros d'amende.

Dans le cas de collecte de données à caractère personnel quel que soit le compte :
- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal)** : le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Si le compte a été détourné pour usurper votre identité :
- **Usurpation d'identité par voie de télécommunication (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

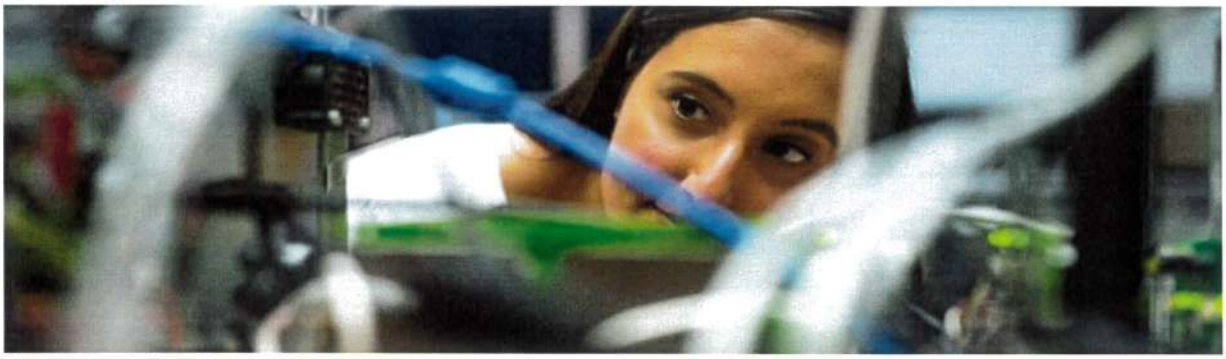
RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 3.0

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 3 : L'importance de réaliser un audit en entreprise



16 Février 2021 Systup

L'audit informatique peut être considéré comme le processus de collecte et d'évaluation des informations. Il permet de déterminer si un système informatique maintient l'intégrité des données et permet d'atteindre efficacement les objectifs de l'entreprise.

Alors que la dépendance des entreprises à l'égard des systèmes informatiques continue de croître, les systèmes informatiques sont confrontés à une multitude de menaces de plus en plus variées.

Il est donc important de fournir un environnement garanti pour le contrôle des risques de l'entreprise.

Pourquoi un audit informatique est-il nécessaire ?

Dans le monde digital dans lequel nous vivons aujourd'hui, l'utilisation des ordinateurs est devenue assez importante. Cela engendre de nombreux problèmes, ce qui augmente encore davantage la cybercriminalité.

Avec l'utilisation massive des systèmes informatiques et les grandes quantités de données stockées sur ces systèmes, il est important que les systèmes informatiques et les données qui y sont stockés soient fiables et sûrs.

Quels que soient la taille et le type de votre entreprise, un audit offre des informations cruciales sur les fonctionnalités du système informatique. Ainsi que les risques de sécurité potentiels et les différentes solutions envisageables.

Les objectifs de l'audit informatique

L'audit informatique consiste en l'identification et l'évaluation des risques informatiques dans une entreprise. Il englobe donc généralement les risques liés à l'intégrité, à la confidentialité et à la disponibilité de l'infrastructure et des processus informatiques.

Des risques supplémentaires : notamment l'efficacité, l'efficience et la fiabilité des systèmes informatiques, peuvent également être résolus par l'identification et l'évaluation régulières des risques dans une entreprise.

Les principaux objectifs d'un audit informatique sont les suivants :

– Évaluer les systèmes et les processus en place qui sécurisent les données de l'entreprise.

– Déterminer les risques qui pèsent sur les actifs informationnels d'une entreprise. Aider à identifier les méthodes permettant de minimiser ces risques.

– S'assurer que les processus de gestion de l'information sont conformes aux lois, politiques et normes spécifiques aux systèmes de l'information.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

– Déterminer les inefficacités des systèmes informatiques et de la gestion associée.

Les étapes du processus d'audit

Une mission d'audit informatique nécessite une bonne préparation. Afin de délimiter le champ d'investigations il est nécessaire de déterminer un champ d'études. En ce sens, elle est susceptible de procéder à un prédiagnostic afin de préciser les questions que l'audit devra traiter.

Voici le processus de réalisation de l'audit informatique en 4 étapes :

1. Définition du périmètre de l'action d'audit à engager

Il s'agit ici du processus d'identification des risques, d'évaluation des risques et de prise de décision visant à réduire les risques à un niveau suffisant.

2. Planification de la mission et suivi de la démarche après validation de la proposition commerciale

Les étapes à suivre en vue de l'élaboration d'un plan d'audit sont les suivantes :

– Faire l'inventaire des systèmes d'informations utilisés dans l'organisation et les classer par catégories.

– Déterminer lesquels des systèmes ont un impact sur les fonctions ou les actifs critiques.

– Évaluer les risques qui affectent ces systèmes et la gravité de l'impact sur l'entreprise.

– Sur la base de l'évaluation ci-dessus, décider de la priorité, des ressources, du calendrier et de la fréquence de l'audit.

3. La collecte des preuves et la réalisation de tests

Afin de soutenir le jugement et les conclusions de l'auditeur, il s'agit d'avoir des preuves pertinentes, compétentes et suffisantes concernant l'organisation, le programme, l'activité ou la fonction faisant l'objet de l'audit.

4. Élaboration du rapport sur les résultats de l'audit informatique

Les auditeurs documentent de manière adéquate les preuves d'audit dans des documents de travail, y compris la base et l'étendue de la planification, le travail effectué et les résultats de l'audit.

Faire appel à un partenaire de confiance pour vous aider dans la réalisation de vos audits informatiques

L'audit informatique est donc essentiel pour les sociétés et les entreprises qui cherchent à protéger leur système informatique ainsi que leurs données et informations précieuses. Ainsi, si votre entreprise a du mal à faire face aux risques potentiels, l'audit informatique peut être la solution idéale pour vous.

La réalisation d'un audit informatique nécessite des connaissances techniques importantes. Chez Systup, nous vous apportons notre expertise afin de vous garantir un service de qualité.

Vous êtes une PME ou TPE qui souhaite évaluer et renforcer son système informatique ? Nous vous invitons à nous contacter dès aujourd'hui. Basée en Île-de-France, notre équipe d'experts se tient à votre disposition pour vous aider.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 4 : Les collectivités face aux enjeux de cybersécurité

SAVIEZ-VOUS QUE

30 %

des collectivités territoriales ont déjà été victimes d'un rançongiciel ?

Étude du Clusif, juin 2020

Les rançongiciels (*ransomware* en anglais) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.
*Source : **www.cybermalveillance.gouv.fr***

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

QUELS SONT LES IMPACTS ?

DIRECTS

Vol de données, chiffrement des données, interruption des services administratifs durant plusieurs jours voire plusieurs semaines.

INDIRECTS

Coûts financiers de rétablissement des services numériques, atteinte à la réputation, conséquences juridiques, etc.

QUE FAUT-IL PROTÉGER ?

DES DONNÉES

Données d'état civil, données personnelles liées aux prestations sociales, données financières, etc.

DES SERVICES

Services en ligne de paiement de contravention, de déclaration d'imposition, de cantine scolaire, d'inscription scolaire, etc.

DES SYSTÈMES & DES INFRASTRUCTURES

Systèmes d'information et de communication, réseaux d'énergie, etc.

En 2020, les signalements d'attaques par rançongiciel ont été multipliés par 3,5 par rapport à 2019. Toutes les collectivités sont concernées, quelle que soit leur taille.

Source : ANSSI

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

ÉVOLUTION DU CADRE RÉGLEMENTAIRE

MAI 2010 *(revisé en 2014)*
Le référentiel général de sécurité (RGS) fixe le premier cadre français de la confiance numérique pour les téléservices et au sein de l'administration.

DÉCEMBRE 2013
La loi de programmation militaire (LPM) garantit la protection des activités d'importance vitale.

AVRIL 2016 (entré en vigueur le 25 mai 2018)
Le Règlement général sur la protection des données (RGPD) responsabilise les acteurs publics et privés quant à la protection des données personnelles.

JUILLET 2016
La directive *Network and Information Security* (NIS) garantit la protection des services essentiels au sein de l'Union européenne.

OCTOBRE 2016
La loi pour une République numérique (LRN) introduit de nouvelles dispositions relatives à l'*Open data* et confirme les dispositions du RGPD en matière de protection des données personnelles.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

QUELS SONT LES OBJECTIFS DE CES RÉGLEMENTATIONS ?

Renforcer la confiance des usagers dans les services numériques.

Garantir la protection des données personnelles et des infrastructures qui les hébergent.

Renforcer la sécurité des activités d'importance vitale et des services essentiels.

SAISISSEZ-VOUS DE L'ENJEU CYBER !

Les collectivités territoriales sont responsables de la sécurité des données qu'elles traitent et de leurs services numériques vis-à-vis des autorités et des citoyens.

Les normes de cybersécurité et de protection des données instaurent une **logique de prévention des risques**. Elles impliquent une mise en conformité permanente et dynamique. Les collectivités doivent donc démontrer qu'elles offrent un niveau optimal de protection.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

QUELLES SONT LES MESURES GÉNÉRALES À METTRE EN PLACE ?

CADRE JURIDIQUE

À SÉCURISER : TÉLÉSERVICES
TEXTE RÉGLEMENTAIRE ASSOCIÉ : RGS

- ✓ Analyse de risques et définition des mesures de sécurité adaptées aux enjeux et aux menaces
- ✓ Homologation de sécurité du téléservice
- ✓ Suivi opérationnel et amélioration continue

À SÉCURISER : DONNÉES PERSONNELLES
TEXTE RÉGLEMENTAIRE ASSOCIÉ : RGPD

- ✓ Nomination d'un délégué à la protection des données
- ✓ Établissement d'un registre de traitement
- ✓ Analyse d'impact lorsqu'un traitement peut impliquer un risque élevé pour les droits et les libertés des personnes concernées
- ✓ Mise en place des clauses relatives à la protection des données personnelles avec ses fournisseurs et ses sous-traitants
- ✓ Notification des violations de données personnelles

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

À SÉCURISER : SYSTÈMES D'INFORMATION D'IMPORTANCE VITALE OU ESSENTIELS
TEXTES RÉGLEMENTAIRES ASSOCIÉS : LPM & DIRECTIVE NIS

- ✓ Définition d'une politique de sécurité des systèmes d'information
- ✓ Cartographie des systèmes d'information
- ✓ Analyse de risques des activités d'importance vitale ou des services essentiels
- ✓ Homologation des systèmes d'information
- ✓ Audit de sécurité

Des services et des produits qualifiés par l'ANSSI permettent de répondre à certaines exigences règlementaires comme celles du RGS :
www.ssi.gouv.fr/administration/visa-de-securite

LES FONDAMENTAUX POUR PROTÉGER SES SERVICES NUMÉRIQUES

SOCLE DE SÉCURITÉ
« MESURES D'HYGIÈNE INFORMATIQUE »

Exemples : sauvegardes régulières, gestion des droits d'accès, gestion des mots de passe, dispositifs de chiffrement, cloisonnement des réseaux, application des correctifs et des mises à jour et détection des incidents.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

POUR FAIRE LA DIFFÉRENCE

- Nommer un responsable de la sécurité numérique
- Organiser des formations régulières au bénéfice des agents
- S'entraîner à la gestion d'incidents de type rançongiciel
- Mettre en place des clauses de sécurité avec ses fournisseurs et ses sous-traitants
- Mettre en place un dispositif de gestion de crise et de continuité d'activité en cas de sinistre
- Adhérer à un dispositif de supervision et de réponse à incident

POUR ALLER PLUS LOIN

- *Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation*, ANSSI, 2020.
- Kit de sensibilisation, **www.cybermalveillance.gouv.fr**
- *Cybersécurité : toutes les communes et intercommunalités sont concernées*, Association des maires de France et des présidents d'intercommunalités, 2020.
- *Guide de sensibilisation au RGPD pour les collectivités territoriales*, CNIL, 2019.
- *Attaques par rançongiciels, tous concernés*, ANSSI, 2020.
- Prestataires de sécurité : le label ExpertCyber, **www.cybermalveillance.gouv.fr**
- *Guide pratique pour une collectivité et un territoire numérique de confiance*, Banque des territoires, 2020

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 5 : Piratage informatique : une formation pour sensibiliser les cadres communaux

Tahiti Infos

PAPEETE, le 08/03/2016 - En décembre dernier, une attaque informatique a touché durant une semaine les services du Pays, de l'État et des entreprises polynésiennes. Un mauvais moment qui a causé beaucoup de dégâts. Aujourd'hui, les communes ne veulent pas que leurs systèmes informatiques rencontrent le même problème, d'où la nécessité de mettre en place une formation sur la sécurité des systèmes informatiques. Formation qui s'est tenue aujourd'hui, dans les locaux du Centre de gestion et de formation.

L'informatique est un milieu assez sournois si on ne prend pas le temps de sécuriser son système. Partout dans le monde, des pirates – que l'on surnomme hackers dans le langage informatique – créent des virus conçus pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés "*hôtes*".

Ces virus peuvent perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Ils peuvent se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et les CD-ROM, les clés USB, etc.

En décembre dernier, une attaque informatique de grande ampleur a touché les services du Pays, de l'État et des entreprises du fenua, durant une semaine, créant une panique générale puisque plusieurs dossiers confidentiels ont été impactés.

Fort heureusement, les communes ont été épargnées, mais cette mésaventure laisse planer le doute quant à l'utilisation d'un matériel informatique. D'où la nécessité pour les communes de mettre en place une formation sur la sécurité des systèmes d'information.

UNE JOURNÉE POUR TOUT ASSIMILER

La formation s'est tenue aujourd'hui dans les locaux du Centre de gestion et de formation (CGF), sous la houlette de Patrick Le Guyader, conseiller en entreprise. Elle était destinée aux cadres communaux. "C'est à eux par la suite de prendre les mesures nécessaires pour appliquer ce qu'ils ont appris", explique-t-on du côté du CGF.

Durant plus de six heures, quatorze stagiaires ont appris plusieurs techniques qui leur permettront de sécuriser leur parc informatique. "Lorsque l'on va sur une page internet, il faut déjà savoir qu'il n'y a aucune sécurité. Lorsque vous allez sur un site comme Google par exemple, vous êtes surveillés avec le phénomène de cookies. À chaque fois que vous vous êtes connectés, on sait que vous êtes venus tel jour, à telle heure et on définit votre profil, si vous êtes un joueur de golf ou de tennis, si vous chaussez du 43 ou si vous avez fait une commande d'achat sur des sites internet. Il y a ce que l'on appelle la traçabilité permanente, donc là, aucune protection de vos libertés individuelles", détaille Patrick Le Guyader. "Une fois que vous vous êtes connectés sur des sites inconnus, c'est la porte ouverte. Il faut dans l'entreprise ou dans la mairie, définir les droits d'usage. Par exemple, interdire de parler de ce qui se passe

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

dans les mairies sur les réseaux sociaux, sur Google, par courrier électronique. On porte atteinte à la liberté des données et de la propriété des individus."

La formation a été déclinée en trois séquences : les aspects législatifs et réglementaires, les risques concernant les courriers électroniques et enfin la nécessité d'avoir un mot de passe alphanumérique.

Pour les stagiaires, cette formation est une aubaine. "On n'est pas forcément formés dans tous les domaines et c'est vrai que maintenant, on parle beaucoup d'E-administration en métropole. Chez nous, c'est encore récent et vu l'éloignement des différentes communes en Polynésie, je pense qu'on va être amenés à faire un petit peu plus d'E-administration ou de la dématérialisation d'actes dont notamment la transmission des actes communaux à la subdivision administrative ou au Haut-commissariat", souligne Maireraurii Leverd, directrice générale des services dans la commune de Bora Bora.

À Fa'a'a, des mesures concrètes ont déjà été prises. "Les clés USB sont autorisées certes, mais suivant un processus bien défini, c'est soumis à autorisation. On n'y accède pas comme cela, donc il y a tout ce contrôle de sécurité, l'échange des fichiers, la constitution des fichiers", explique Éric Chan, responsable informatique.

LE CENTRE DE GESTION ET DE FORMATION A ÉGALEMENT ÉTÉ INFECTÉ L'AN DERNIER

Depuis cette mésaventure, la sécurité des données informatiques a été renforcée. "Les mots de passe doivent être alphanumériques, il faut que le mot de passe contienne au moins huit caractères et ils changent tous les six mois. Les sites internet sur lesquels naviguent les employés du CGF, sont contrôlés. J'ai bloqué l'accès à certains sites, comme les réseaux sociaux ou encore You Tube", précise Moana, informaticien au CGF. "On a revu notre règlement intérieur des agents du CGF, on a mis une charte de bonne conduite et chacun en a pris connaissance. On a sécurisé nos réseaux périphériques de bases de données internes, on a investi dans des disques durs sophistiqués", complète Bertrand Raveneau, directeur général du CGF.

Tous les mois, des formations sont également mises en place dans leurs locaux et contrôler les stagiaires n'est pas une tâche évidente. "Les stagiaires ne peuvent pas utiliser leurs clés USB, le CGF met à leur disposition des clés USB CGF. Lorsqu'une formation a lieu, le stagiaire récupère les données de cette formation et si le stagiaire arrive avec sa clé, le CGF contrôle que sa clé n'est pas vérolée. Les stagiaires ne peuvent pas se connecter sur les PC, mais ils peuvent se connecter sur internet pour consulter leurs mails", explique le directeur général du CGF.

Au vu de l'importance à sensibiliser le personnel communal, "s'il le faut, avec le prestataire, il y aura d'autres sessions qui sont prévues, soit cinq séquences possibles", conclut Bertrand Raveneau.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 6 : Les 10 astuces pour sécuriser votre poste de travail en moins de 5 minutes

En 2015, les cyber-attaques se sont multipliées rythmant ainsi l'actualité IT. En effet, le monde de la sécurité IT n'a pas cessé de relater les vols de données subis par les entreprises avec notamment le journal Le Monde qui a perdu pendant plusieurs heures le contrôle de son compte Twitter, ou encore la chaîne publique TV5 Monde qui est victime d'un piratage qui touche à la fois son site Internet, mais également ses comptes Facebook et Twitter, ainsi que ses onze canaux de diffusion.

Si les pirates redoublent de ruses pour nous piéger, il existe toutefois quelques manipulations simples à réaliser et d'une rapidité déconcertante pour protéger et sécuriser vos données. Apprenez à sécuriser votre poste de travail en 10 étapes pour barrer la route aux pirates informatiques.

1. Choisir un mot de passe sécurisé pour votre session utilisateur

C'est en effet le b.a.-ba de la sécurité informatique, et qui est malheureusement que trop pris à la légère. Si vous oubliez votre ordinateur portable dans le train ou que vous vous le fassiez dérober, n'importe qui pourrait accéder à vos documents, qu'ils soient personnels ou professionnels. De la même manière, un collègue de travail malveillant avec lequel vous seriez en conflit pourrait également se connecter à votre session dès votre dos tourné.

Si mettre un mot de passe à votre appareil (smartphone, tablette) et à votre session est déjà un premier pas, encore faut-il que celui-ci soit sécurisé !

Voici quelques conseils pour construire un mot de passe sûr :

- Optez pour un mot de passe long : plus il y a de caractères, plus un mot de passe sera difficilement déchiffrable
- Donnez-lui un niveau de sécurité élevé : mixez lettres, chiffres et espaces

La première chose est surtout de bannir tous les mots de passe trop faciles et trop utilisés, consultables dans la liste des 25 pires mots de passe de l'année 20151. Autant dire qu'ils disposent d'un niveau de sécurité proche de zéro…
Attention, construire un mot de passe en accumulant des majuscules, des minuscules et des chiffres sans aucun sens va être très compliqué à retenir, et vous risquez d'être tenté de le noter quelque part… Imaginez plutôt une phrase dans votre tête, conservez la première lettre de chaque mot et ajoutez quelques chiffres : ce sera plus facilement mémorisable ! Enfin, pensez à utiliser un mot de passe différent pour chaque utilisation.

2. Utiliser un compte utilisateur sur votre ordinateur plutôt qu'un compte administrateur

Si vous êtes connecté avec un compte administrateur, votre machine ne va pas vous redemander vos identifiants quand vous souhaitez télécharger un programme, l'installation se fera automatiquement. À contrario, si vous utilisez une session avec un compte utilisateur, vous devrez à chaque fois renseigner les codes administrateurs pour qu'un logiciel soit installé. Cela permet d'éviter l'installation de programmes malveillants à votre insu.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

3. Laisser le firewall actif

Que vous utilisiez une machine sous iOS ou sous Windows, les deux systèmes d'exploitation disposent tous deux d'un pare-feu, ou firewall. Il permet de bloquer l'accès à votre ordinateur par des utilisateurs et des logiciels malveillants depuis Internet et/ou un réseau local, mais également d'empêcher votre poste d'envoyer des programmes, nuisibles et infectés, à d'autres machines.

4. Installer un anti-virus

Il est important d'équiper votre poste d'un anti-virus puissant, mais surtout de le tenir à jour et de le paramétrer afin qu'il assure des scans réguliers de votre poste.

5. Effectuer les mises à jour autant que faire se peut

Les mises à jour permettent certes d'enrichir en fonctionnalités un système ou une application ou encore de corriger des bugs, mais elles permettent surtout de combler des failles de sécurité. Aussi, vous devez systématiquement effectuer les mises à jours système et applicatives. Vous vous assurez d'une part d'avoir un logiciel le plus complet possible, mais aussi un environnement des plus sécurisé.

Document 6 : p.1 / 3

6. Chiffrer les dossiers qui contiennent des données confidentielles

Protéger votre session avec un mot de passe sécurisé (étape 1) permet d'éviter que quelqu'un se connecte à votre place. Si cette étape est nécessaire, elle n'est toutefois pas suffisante. Il suffirait en effet d'installer votre disque dur sur un autre ordinateur pour pouvoir accéder à vos données. Ainsi, pensez à chiffrer les répertoires de travail qui contiennent des données confidentielles. La manipulation est très simple : clic droit sur le dossier -> Propriétés -> Onglet Général, bouton Avancé -> et cochez « Chiffrer le contenu pour sécuriser les données ». Quelques clics suffisent à protéger vos documents

7. Avoir un comportement prudent

Aussi fabuleux soit-il, Internet reste un outil dangereux pour la sécurité de vos données, il faut donc que vous naviguiez de façon avisée. Prenez garde aux sites web que vous visitez, vérifiez les certificats de sécurité des pages de paiement, et contrôlez la fiabilité des sites Internet avant tout téléchargement.
D'autre part, ne laissez jamais votre appareil sans surveillance, d'autant plus avec votre session déverrouillée.

8. Se protéger du phishing

Véritable piège pour les internautes, le phishing est une pratique malveillante qui consiste à soutirer des données personnelles (identifiants de connexion, mots de passe, numéro de carte bancaire,...). Les attaques sont de plus en plus nombreuses : plus de 2 millions de français en ont fait les frais en 2015, soit 100 fois plus qu'en 2013. En pratique, vous recevez un e-mail, souvent personnalisé, de la part d'un organisme financier (une banque) ou public (CAF, Assurance Maladie,...) ou encore d'une entreprise (FAI, EDF...) qui vous demande de mettre à jour vos informations personnelles. Un lien vous renvoie vers un site frauduleux qui permet aux pirates de

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

récupérer ces données. Prenez donc garde à ce genre d'e-mails, des fautes d'orthographe vous mettront la puce à l'oreille.

9. Désinstaller/désactiver les programmes superflus

Supprimez les logiciels et applications dont vous ne vous servez pas et qui ne sont pas indispensables, cela fera moins d'éléments à mettre à jour, moins de failles de sécurité et moins de portes d'entrée pour les hackers.

10. Se méfier des supports de stockage amovibles

Les clés USB sont des nids à virus et permettent de propager très facilement des malwares une fois connecté à votre ordinateur. N'en utilisez qu'une seule dont vous êtes sûr de la fiabilité, et préférez le stockage de données dans le cloud via un prestataire professionnel, français de préférence.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 7 : Cyberattaques : quand les collectivités cherchent la parade

Parce qu'elles manipulent de nombreuses données personnelles et sensibles sur leurs administrés et qu'elles ont de forts enjeux de continuité de service public, les cyberattaques visent de plus en plus de collectivités. Des grandes métropoles aux plus petites mairies, comment faire face à ces menaces ? État des lieux.
Certains experts en cyber considèrent que la cyberattaque contre la ville de Baltimore aux États-Unis en mai 2019 est un événement marquant des menaces cyber contre les collectivités. Les montants de rançon et de remédiation élevés, la couverture médiatique ou encore le volume de postes concernés, le cas avait en effet marqué les esprits. Et semble avoir fait appel d'air, puisque les exemples se multiplient depuis, à une échelle mondiale.

Cyberattaques et collectivités : une menace à l'échelle internationale

Selon une étude de 2020, 44% des attaques de ransomwares visaient des municipalités. Des attaques par ransomwares qui se complexifient encore pour les victimes. En septembre 2020, des cyber-criminels mettaient en ligne 20 gigaoctets de données volées à la métropole d'Aix-Provence-Marseille. S'y trouvaient des noms d'agents et leurs matricules, ou encore deux fichiers avec 23 000 adresses électroniques associées à des noms. Une fuite de données sensibles qui a mis un coup de projecteur sur une nouvelle forme d'intimidation, qui consiste à menacer de faire fuiter les données pour pousser au paiement d'une rançon.
Et la menace est mondiale. En juillet 2021, l'administration du district d'Anhalt-Bitterfeld, en Allemagne, avait été contrainte de ressortir ses fax du placard après une cyberattaque. En Italie, c'est toute la région du Latium qui était impactée au mois d'août, quand un ransomware avait paralysé le data center régional, rendant notamment indisponible la plateforme de réservation pour la vaccination anti-Covid. Du côté des États-Unis, les exemples sont légion. En septembre 2021, le Washington Post n'hésitait d'ailleurs pas à titrer Les ransomwares sèment le chaos sur les villes américaines. De la police de Washington aux écoles du comté de Fairfax, la tendance semble bien installée et touche même les établissements pénitentiaires. Ainsi, en janvier 2022, une prison du Nouveau-Mexique était visée par une cyberattaque, mettant hors service caméras et portes automatiques.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

« Il y a une explosion des attaques par ransomware, confirme Vincent Nicaise, Responsable des partenariats et de l'écosystème industriels chez Stormshield. D'autant plus que certaines collectivités opèrent tant des infrastructures IT classiques que des infrastructures OT, plus sensibles – comme le montre l'exemple de la cyberattaque au Nouveau-Mexique. » Pourtant, communautés de communes et autres mairies ne sont pas connues pour leur trésorerie abondante. Pourquoi alors les cibler ? Pour Philippe Loudenot, administrateur du CESIN, délégué cybersécurité au Conseil régional des Pays de la Loire, ancien fonctionnaire Sécurité des Systèmes d'Information (FSSI) au sein des ministères sociaux, il s'agit le plus souvent d'attaques opportunistes. Mais constituant une menace directe sur le bon fonctionnement des services publics, les cyberattaques impactant les collectivités locales méritent de s'y intéresser.

Le service public mis à mal par les cyberattaques

Si la cybersécurité des collectivités est aussi importante, c'est donc parce qu'une cyberattaque visant une collectivité peut avoir des conséquences diverses, à chaque fois désastreuses. Philippe Loudenot en distingue cinq.

La mise en péril de la continuité du service public, propre aux administrations. Les collectivités dépendent en effet de leurs systèmes informatiques pour administrer un vaste champ de missions, de la cantine scolaire aux réseaux de transports en passant par l'action sociale. Sans accès à leurs données, ces missions sont interrompues ou fortement dégradées.
La fuite, le vol ou la perte de données personnelles est également à considérer, puisque les collectivités ont accès à des données sensibles concernant leurs administrés. Ainsi en mai 2021, des cyber-criminels ont diffusé les données de 1 000 agents du Grand Annecy, dont leurs résultats de tests Covid et leurs coordonnées personnelles, cinq mois après une attaque sur le système informatique de la communauté d'agglomération. En août 2021, c'est le site français de demandes de visa qui était attaqué de la sorte.

La perte de patrimoine informationnel est un autre risque propre aux collectivités. En plus des données qui concernent leurs administrés, « les collectivités sont détentrices d'un patrimoine informationnel important », fait savoir Philippe Loudenot, comme par exemple les données d'état civil, sociales, finances et taxation, etc. En cas de destruction ou de mise à mal de l'intégrité de ces données, la collectivité risque de perdre une partie de son histoire.
L'impact sur l'image de la collectivité est également une conséquence importante. Une cyberattaque, si elle est connue des administrés, pourra avoir un impact négatif sur la confiance des citoyens en la collectivité et ses services. Et ce d'autant plus en période d'élections locales…
Enfin, le risque juridique est à prendre en compte. En cas de faute avérée dans la protection des données personnelles, la collectivité s'expose à des sanctions de la part d'instances étatiques mais aussi des poursuites judiciaires de la part des administrés eux-mêmes.

La bourse ou la vie publique
Au niveau de la répartition des menaces, et selon un rapport du Clusif de 2020, une association française dédiée à la sécurité informatique, 30% des collectivités se déclaraient victimes d'un ransomware. Un chiffre à prendre avec du recul tant les cyberattaques passent souvent sous les radars : plus de la moitié des collectivités interrogées affirmaient ne pas communiquer dessus. En 2021, le journal LeMagIt tenait un décompte des villes françaises touchées par un ransomware. Au total, une soixantaine, dont Mitry-Mory, Chalon-sur-Saône, la communauté de communes de l'Est lyonnais, Douai, Villepinte, Erstein, Istres, ou encore Annecy.
Comme le précise l'ANSSI dans un guide dédié, toutes les communes et intercommunalités sont concernées.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Les rançons demandées peuvent être très variables, mais il faut aussi prendre en compte les coûts indirects liés à une attaque

Philippe Loudenot, délégué cybersécurité au Conseil régional des Pays de la Loire, ancien fonctionnaire Sécurité des Systèmes d'Information (FSSI) au sein du ministère de la Santé et des services du Premier ministre

Au niveau des montants des rançons, ceux-ci s'élèvent en moyenne à 836 000 dollars aux États-Unis, contre 130 000 euros en France selon l'ANSSI. « Les rançons demandées peuvent être très variables, mais il faut aussi prendre en compte les coûts indirects », souligne Philippe Loudenot. Car le versement d'une rançon n'est pas la seule perte qui peut être imputée à une cyberattaque. La ville de Chalon-sur-Saône et l'agglomération du Grand Chalon ont par exemple déboursé 550 000 euros pour remettre leurs systèmes informatiques sur pied après une cyberattaque en février 2021. La collectivité n'a pas fait état de paiement de rançon, la somme ayant été entièrement dirigée vers la remédiation – soit la récupération des données et la remise en route du système. Concrètement, cela s'est traduit par la mise en place de nouvelles procédures et par des recrutements pour renforcer les équipes chargées des infrastructures réseaux, des projets techniques et des systèmes de sécurité. Philippe Loudenot évoque également les coûts liés aux salaires versés aux employés au chômage technique ainsi que les coûts de communication nécessaires à la bonne information des administrés. Enfin, les cyber-merdes volant en escadrille, d'éventuelles sanctions peuvent être envisagées si des fautes sont relevées dans la protection des données personnelles : « même si la Commission nationale de l'informatique et des libertés (CNIL) est plutôt dans une logique d'accompagnement ».

Vecteurs de risque et surface d'attaque des collectivités

Une logique d'accompagnement nécessaire à tous les niveaux, tant la surface d'attaque des collectivités locales est étendue, du fait de plusieurs points de fragilité. Aux origines de cette fragilité, un manque certain de budget alloué aux questions de cybersécurité : la plupart des collectivités françaises consacrent moins de 10% de leur budget à la cybersécurité, taux recommandé par l'ANSSI.

Une première conséquence directe : les sources d'infections sont souvent liées au facteur humain. Rien de révolutionnaire ici tant les agents sont régulièrement exposés au phishing. Et l'effort de pédagogie, entre sensibilisation à l'hygiène numérique et formation à la cybersécurité, reste encore à ce jour trop faible.

Un manque de budget qui ouvre également une autre porte d'entrée potentielle aux cyber-criminels avec des postes de travail vieillissants, qui utilisent des systèmes d'exploitation obsolètes souvent en retard en matière de mises à jour. Et le champ à couvrir et protéger est en perpétuelle extension : les collectivités locales ont équipé leurs agents en smartphones, tablettes et PC portables. Autant de portes d'entrées additionnelles avec ces flottes d'appareils connectés dont les mots de passe sont souvent peu sécurisés, parfois affichés dans les bureaux, et que les agents ne modifient que très rarement.

Les réseaux informatiques (et opérationnels) que gèrent les collectivités sont un des autres points de fragilité. En cause, des systèmes souvent à plat, sans segmentation réseau, et donc sensibles aux attaques latérales. Une cyberattaque contre un des services de la collectivité peut donc contaminer les autres, « grâce » à leur interconnexion. Et une fois implanté, le malware peut rester en sommeil pendant un moment, avant d'être activé au moment le plus opportun par les cyber-criminels, comme du côté de Gloucester au Royaume-Uni, touché en janvier 2022.

Autre point de vulnérabilité : l'attaque malveillante interne, soulève Philippe Loudenot, qui évoque « une curiosité malsaine qui pousserait un agent à accéder à des informations confidentielles » ou encore un ancien agent mécontent, dont les accès aux systèmes informatiques n'ont pas été révoqués.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Cybersécurité des collectivités : des solutions à long terme

Menacées de l'intérieur comme de l'extérieur, les administrations sont-elles donc condamnées à subir des vagues d'attaques incessantes ? Si une certaine lourdeur administrative peut empêcher l'adaptation et la flexibilité nécessaires à une meilleure protection face aux risques cyber, il existe toutefois des solutions. En France, les cyberattaques visant les collectivités sont du ressort conjoint de l'ANSSI et du département de cybercriminalité de la gendarmerie nationale. En cas de ransomware, les recommandations de ces institutions demeurent classiques, précise Philippe Loudenot : « ne pas payer la rançon afin de ne pas encourager les futurs cyber-criminels, déposer plainte et faire remonter l'information ».

Mais l'adage « mieux vaut prévenir que guérir » s'applique aussi en l'espèce. Il faut donc surtout que les collectivités modifient leur approche globale en matière de cybersécurité. L'objectif ? P arvenir à la mise en place d'une protection à long terme, qui passe par une série de mesures.

La sensibilisation en est la plus évidente. « Il faut mettre tout le monde à niveau sur les gestes de base d'hygiène numérique », explique Philippe Loudenot. Mettre en place des mots de passe robustes, les changer régulièrement, ne pas les laisser traîner sur des post-it sur son bureau, se méfier des liens reçus… Des réflexes simples (basiques) mais qui restent encore à intégrer, reconnaît Philippe Loudenot. « On en est encore loin, déplore-t-il. Le discours est tronqué car on parle essentiellement des menaces et les collectivités ne se sentent pas touchées. Il faut parler des impacts. Cela touche tout le monde de savoir qu'on ne sera pas capable d'assurer la continuité de son service public. » Pour l'expert, il faut transformer la perspective : « ce n'est pas 'si' mais 'quand' une collectivité se fera attaquer. Qu'est-ce que l'on met en place ? Quelles manières alternatives de travailler ? ». Un retard de sensibilisation que remarque également Vincent Nicaise. Il souligne que dans le cadre du programme France Relance, l'État français peut prendre en charge jusqu'à 100% du diagnostic au sein d'une collectivité afin que celle-ci fasse le point sur son niveau et ses besoins. Et pour aller plus loin, de nombreux guides pratiques ont enfin été édités par le gouvernement autour de la cybersécurité des services publics. Tout début 2022, l'Agence nationale de la cohésion des territoires (ANCT) s'est associée à Cybermalveillance.gouv.fr, la Gendarmerie nationale et l'Association des maires de France (AMF) pour organiser un webinaire d'information, de prévention et de solutions pour les collectivités locales.

Le discours est tronqué car on parle essentiellement des menaces et les collectivités ne se sentent pas touchées. Il faut parler des impacts. Cela touche tout le monde de savoir qu'on ne sera pas capable d'assurer la continuité de son service public

Philippe Loudenot, délégué cybersécurité au Conseil régional des Pays de la Loire, ancien fonctionnaire Sécurité des Systèmes d'Information (FSSI) au sein du ministère de la Santé et des services du Premier ministre

En parallèle de la sensibilisation, les collectivités doivent également mettre en place des solutions de protection adaptées. Solutions endpoint pour protéger les postes de travail, firewalls pour sécuriser les réseaux, solutions de chiffrement pour assurer l'intégrité des données, les outils sont divers et variés. Mais elles viennent forcément avec un certain coût.

En France, l'ANSSI a pris conscience de ces enjeux depuis plusieurs années et avait déjà proposé un budget conséquent pour accompagner les collectivités, à hauteur de 60 millions d'euros sur 2021 et 2022. En ce début d'année 2022, les premiers bénéficiaires du programme France Relance arrivent à la fin du parcours de cybersécurité (sur la partie audit) et devraient accéder au

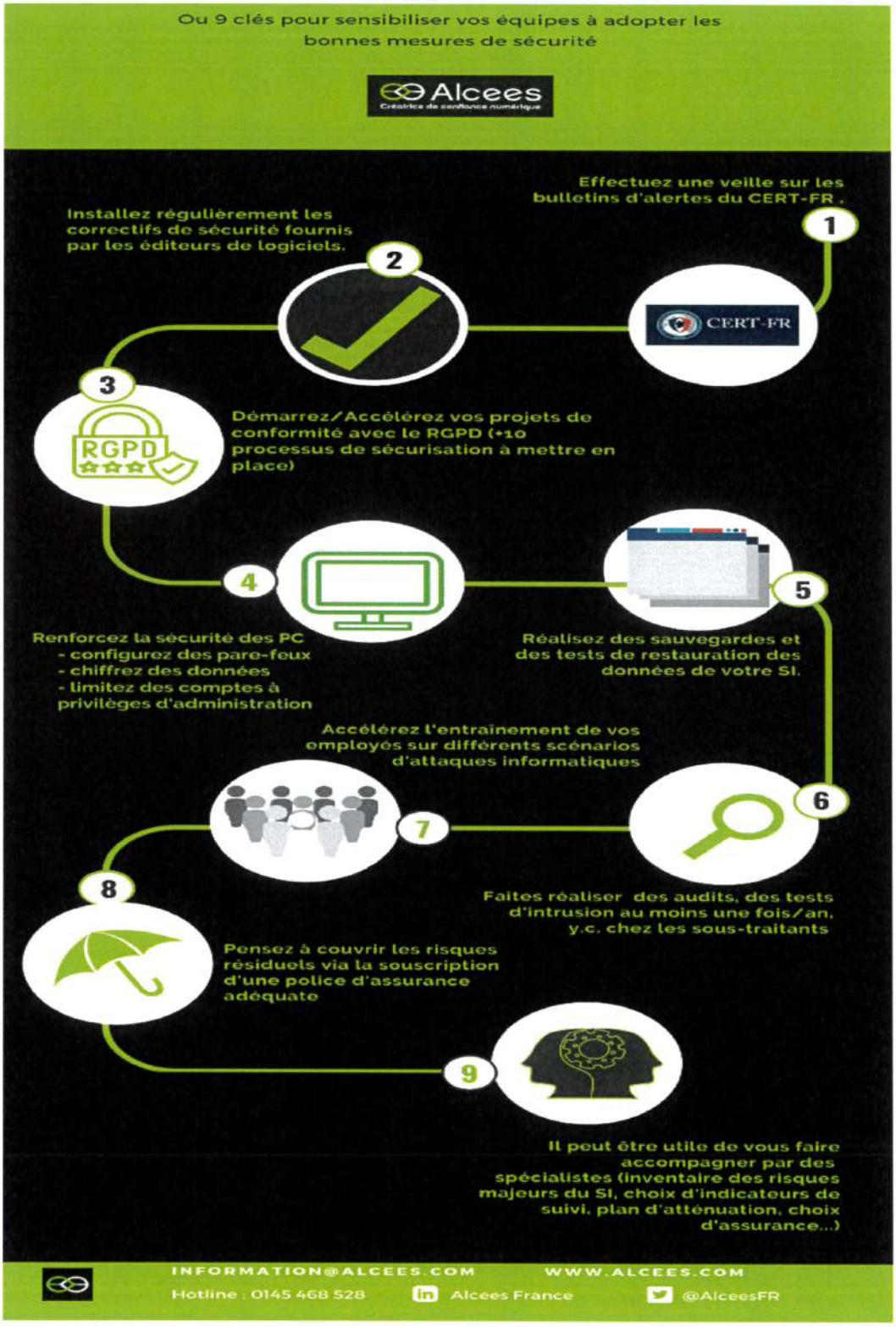
Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

plan de co-financement (jusqu'à 70%, dans le cadre du programme). Ainsi, 2022 devrait être (enfin ?) l'année de la sécurisation des systèmes.
Autre approche efficace : la mise en place d'un système de sauvegarde. Ainsi, la collectivité de Chalon-sur-Saône fait figure de bon élève : les sauvegardes automatiques de données effectuées à J-1 ont permis à la collectivité de remettre en route ses systèmes sans pertes de données à la suite de l'attaque subie en février 2021. Un système efficace qui « devrait systématiquement être mis en place, recommande Philippe Loudenot, mais c'est loin d'être le cas ».
Côté français, l'accent est également mis sur la constitution d'un réseau de référents locaux. Ce réseau s'appuiera sur des référents cybersécurité afin de rester à jour dans la connaissance des fragilités et alertes émises par l'ANSSI et le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques). La création d'un CSIRT régional (Computer Security Incident Response Team) est d'ailleurs en cours, en parallèle de l'annonce de la création d'un réseau de RSSI territoriaux, annoncée lors du FIC 2021. Enfin, il est également important de noter que le groupement d'intérêt public cybermalveillance.gouv.fr a mis en place un label Ville Cyber Responsable pour distinguer les villes engagées dans un plan d'action pour lutter contre les cyberattaques.

Autant d'initiatives qui font que « aujourd'hui, les élus prennent conscience que la cybersécurité de leurs collectivités n'est pas un non-sujet », estime Philippe Loudenot. Ça tombe bien, il y a du pain sur la planche.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

Document 8 : 9 conseils pour maintenir un SI robuste et sécurisé



Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

1 | Effectuez une veille sur les bulletins d'alertes du CERT-FR

La plupart des logiciels et matériels utilisés dans le système d'information d'un établissement de santé nécessitent une mise à jour périodique pour assurer leur sécurité et ajouter des fonctionnalités.

La mise à jour du logiciel est essentielle pour maintenir un système d'information santé sécurisé, car bon nombre de ces mises à jour corrigent les vulnérabilités nouvellement découvertes dans le produit. Le CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, publie sur son site web des alertes et des avis sur les vulnérabilités découvertes dans des logiciels et matériels et donne, lorsque cela est possible, des moyens de s'en prémunir.

2 | Installez régulièrement les correctifs de sécurité fournis par les éditeurs de logiciels

Qu'il s'agisse de logiciels, d'application ou de systèmes d'exploitation, il est vivement recommandé de surveiller les correctifs et mises à jour critiques et urgentes qui nécessitent une attention immédiate. Les messages des fournisseurs concernant ces correctifs et mises à jour doivent être surveillés et traités dès que possible.

3 | Démarrez/Accélérez vos projets de conformité avec le RGPD pour sécuriser les données sensibles de santé et les droits des utilisateurs

Un vol ou une perte de données médicales peut avoir des impacts très préjudiciables sur l'image de l'établissement de santé, et surtout sur le patient concerné. Cette mésaventure d'une ampleur jamais rencontrée en France, est arrivée à 28 laboratoires d'analyses médicales sous licence avec Dedalus France, éditeur de logiciels pour les établissements de santé (publication des noms, coordonnées (adresse postale, téléphone, email), numéros de sécurité sociale parfois accompagnés d'indications sur le groupe sanguin, le médecin traitant ou la mutuelle, ou encore de commentaires sur l'état de santé (dont une éventuelle grossesse), des traitements médicamenteux, ou des pathologies (notamment le VIH), de près de 500 000 personnes en France, dont un millier de militaires) le 23 février, suite à un piratage informatique.

Les attaques informatiques se multiplient actuellement contre les établissements de santé en France. Des cyberattaques par rançonlogiciel ont ainsi paralysé les hôpitaux de Dax et de Villefranche-sur-Saône les 8 et 15 février dernier. Les préjudices pour les patients lésés sont mesurables.

Assurer la sécurité des données de santé doit donc constituer une exigence à part entière pour l'établissement de santé. A ce titre, le règlement général sur la protection des données (RGPD) peut être vu comme une opportunité pour améliorer les pratiques de sécurité des professionnels de santé, voire limiter au maximum la survenance des risques de piratages informatiques.

4 | Renforcez la sécurité des PC

Les données de santé occupent une place majeure dans le patrimoine informationnel d'un établissement hospitalier.

L'essor du risque pandémique et de la mise en place des suivis de patients à distance renforcent la nécessité de collecter, d'analyser, d'exploiter, de conserver ou d'échanger avec différents acteurs du système de santé, jusqu'à 50 fois plus de données médicales brutes qu'avant les années 2020.

Que ce soit à des fins de prévention, d'accélération de la recherche médicale ou du traitement de pathologies à risque létal aggravé, la pertinence de l'application des techniques de big data ou d'intelligence artificielle au domaine santé, se confirme plus que jamais, *a fortitori* dans le contexte de gestion de crise sanitaire coronavirus SARS-Cov-2.

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf

L'intérêt stratégique à disposer de gisements de SI santé partagés se matérialise également dans de nombreux projets nationaux comme la Plateforme des données de santé (Health Data Hub) ou comme le SI « Vaccin Covid ».

Mais la convoitise des cybercriminels pour les dossiers médicaux gagne en popularité et en variété dans les années 2020. Rentable (les estimations sont difficiles, mais le ransomware Ryuk par exemple, aurait généré 150 millions de dollars de revenus cumulés depuis ses débuts en 2018), le marché du rançonlogiciel-comme-un-service, est de l'avis de plusieurs experts en cybersécurité, appelé à croître.

5 | Réalisez régulièrement des sauvegardes et des tests de restauration

Les données de santé occupent une place majeure dans le patrimoine informationnel d'un établissement hospitalier.

L'essor du risque pandémique et de la mise en place des suivis de patients à distance renforcent la nécessité de collecter, d'analyser, d'exploiter, de conserver ou d'échanger avec différents acteurs du système de santé, jusqu'à 50 fois plus de données médicales brutes qu'avant les années 2020.

Que ce soit à des fins de prévention, d'accélération de la recherche médicale ou du traitement de pathologies à risque létal aggravé, la pertinence de l'application des techniques de big data ou d'intelligence artificielle au domaine santé, se confirme plus que jamais, *a fortitori* dans le contexte de gestion de crise sanitaire coronavirus SARS-Cov-2.

L'intérêt stratégique à disposer de gisements de SI santé partagés se matérialise également dans de nombreux projets nationaux comme la Plateforme des données de santé (Health Data Hub) ou comme le SI « Vaccin Covid ».

Mais la convoitise des cybercriminels pour les dossiers médicaux gagne en popularité et en variété dans les années 2020. Rentable (les estimations sont difficiles, mais le ransomware Ryuk par exemple, aurait généré 150 millions de dollars de revenus cumulés depuis ses débuts en 2018), le marché du rançonlogiciel-comme-un-service, est de l'avis de plusieurs experts en cybersécurité, appelé à croître.

6 | Test intrusion audits de sécurité

Faites réaliser des audits, des tests d'intrusion au moins une fois/an, y compris chez des sous-traitants

7 | Entrainement

Accélérez l'entrainement de vos employés sur différents scénarios d'attaques informatiques.

8 | Couverture des risques

Pensez à couvrir les risques résiduels via la souscription d'une police d'assurance adéquate.

9 | Accompagnement

Il peut être utile de vous faire accompagner par des spécialistes (inventaire des risques majeurs du SI, choix de l'indicateur de suivi, plan d'atténuation, choix d'assurance...

Centre de gestion et de formation – Avenue G.Clémenceau- Immeuble la ora na, 3e étage, Mamao
BP 40 267 – 98713 Papeete – tél. +689 40.54.78.10 – télécopie : +689 40.82.71.89 – concours@cgf.pf