Centre de gestion de la fonction publique territoriale du Rhône et de la Métropole de Lyon

CONCOURS ou EXAMEN de

Technicien Territorial

à titre interne ☐ (1)

à titre externe ☒ (1)

au titre du troisième concours ☐ (1)

Spécialité : Ingénierie, Informatique et Systèmes d'Information.

Épreuve de : Réponse à des questions techniques

Date de l'épreuve : 12/04/2018

Colonne réservée à l'administration

Numéro de copie

Note attribuée (réservé au jury)

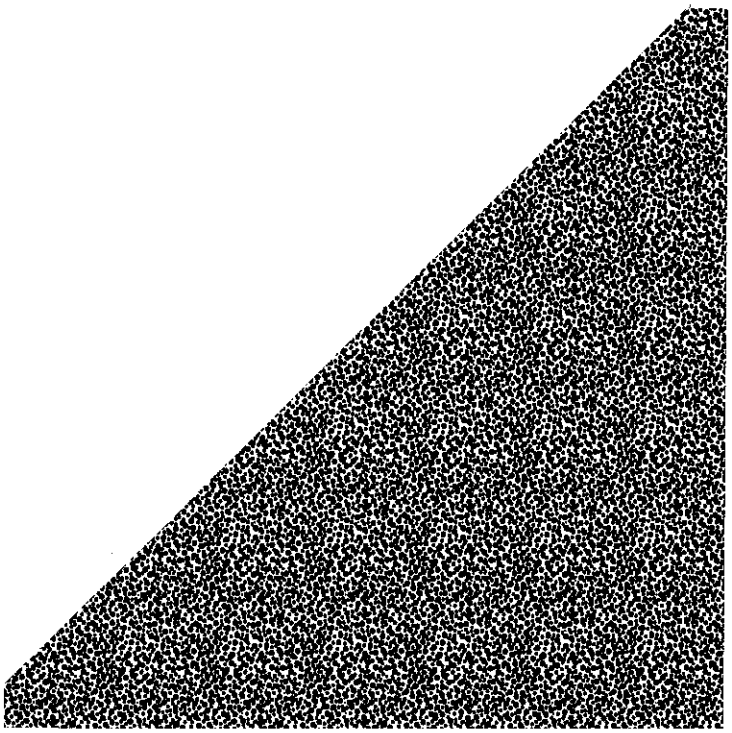
13,75

Question 1 :

Avec des besoins de plus en plus gourmands au niveau des débits, les réseaux de connexion et d'échange de données basés sur les fils de cuivre (ex : ligne SDSL) ne suffisent souvent plus. La fibre optique se développe alors, permettant de transmettre les informations plus rapidement, pour des usages résidentiels ou professionnels. Ces réseaux réseaux de fibre optique se développent grâce au FttH (Fiber to the home) pour la "Fibre au domicile" et au FttO (Fiber to the office) pour la "Fibre au bureau".

En comparant les deux types de réseaux, il apparaît de nombreux avantages à se tourner vers des solutions de FttO pour les collectivités, plutôt que du FttH. Les besoins des professionnels sont en effet très demandeurs de débits élevés pour les transferts de fichiers volumineux. De plus, ces fichiers doivent être transmis rapidement, une interconnexion grâce au VPN peut être une solution pour accélérer ces transferts. Les solutions de FttO permettent ces interconnexions rapides. De même, la connexion FttO est intéressante pour les entreprises et collectivités puisqu'elle permet d'être en lien direct,

(1) Cocher la case correspondante



via une boucle locale dédiée, avec le NRO (Noeud de Raccordement optique) ce qui n'est pas le cas en FttH. Les débits seront alors maximisés, les échanges mieux sécurisés et les flux pouvant être priorisés en réservant une partie importante à la visio conférence par exemple. La souscription à une offre de FttO par une collectivité lui garantit un rétablissement plus rapide en cas de panne, puisque l'opérateur sera organisé pour ce type de contrat. Enfin, il est possible, afin de minimiser les coûts, de s'inscrire dans des réseaux d'initiatives publiques où plusieurs collectivités et/ou entreprises se regroupent en négociant les tarifs.

Question 2.

De nombreux éléments doivent être pris en compte en amont d'un raccordement d'une zone d'activité en très haut débit. Il s'agit tout d'abord d'évaluer les besoins en THD (Très Haut Débit). Un diagnostic peut-être réalisé dans chaque entreprise pour cibler la demande collective. Un appel à la concurrence peut être lancé après s'être assuré d'un maillage possible de la zone d'activité par la fibre. En effet, le raccordement doit pouvoir se faire au réseau de collecte en entrée de la zone. Le réseau de desserte doit être efficace et équipé en infrastructures d'accueil, accessible via des locaux techniques ; ce sont notamment ces éléments qui permettront de mettre en concurrence les opérateurs. Ces derniers devront être en mesure de s'engager à offrir des connexions THD aux entreprises. Une autre préconisation est de connaître l'ensemble des réseaux, les inscrire dans un SIG (Système d'Information Géographique) pour ensuite prévoir et adapter les réseaux de câbles optiques à déployer.

Question 3.

A) Le Règlement Général sur la Protection des Données (RGPD) a été établi au niveau européen afin de protéger les données personnelles des utilisateurs; données divulguées sur Internet notamment.

Au sein des collectivités, les enjeux du RGPD sont multiples. De plus en plus, la dématérialisation et le développement de l'administration en ligne sont présents avec la compilation de nombreuses données nominatives et personnelles. Il est nécessaire de veiller à l'intégrité de ces données face à des cyber attaques en augmentation croissante. L'entrée en vigueur du RGPD au 25 mai 2018 renforcera le respect du traitement des données personnelles de manière générale. Un des enjeux du RGPD est d'instaurer une culture de responsabilisation des collectivités face à la sécurisation, la manipulation et la demande de données personnelles de leurs administrés. Il s'agit de développer des mesures visant à organiser les structures dès la récupération de données personnelles. Les collectivités auront à tenir un registre des traitements réalisés et encadreront les opérations au coeur des prestations de services. De même, le RGPD devrait permettre à la CNIL d'avoir un pouvoir de sanction renforcé dès lors d'un manquement au respect du règlement.

B) La collectivité, dans une logique d'application et de respect du RGPD, devra réduire les risques des travailleurs nomades grâce à un pistage des accès des utilisateurs. Les travailleurs nomades sont en effet plus sensibles aux cyber attaques que les autres. L'ensemble des utilisateurs devront avoir des comptes davantage sécurisés via une authentification forte et un serveur de rebond. Une sensibilisation et une formation des agents est requise pour éviter ou réduire les tentatives de cyber attaques par hameçonnage et e-mails frauduleux. Des processus automatisés de sécurisation pourront être développés afin de pallier à certaines failles comme la gestion de la vie des identités à renouveler. Autre changement majeur avec la mise en place du RGPD sera la nomination d'un Data protection Officer. Cela sera obligatoire pour les collectivités. Cette personne devra conseiller le responsable des

traitements de collecte, informer et former les agents sur les obligations et la vigilance en matière de manipulation de données personnelles. Il pourra conseiller la collectivité sur les bonnes pratiques à adopter. Pour les collectivités petites et moyennes, la mutualisation du Data protection Officer sera nécessaire pour absorber les coûts engendrés. Cela pourra se faire en se rapprochant des SMI (Structures de Mutualisation Informatique). Elles proposent en effet un accompagnement des collectivités dans le numérique. De même, les collectivités telles que les communautés d'agglomération, métropoles et communautés urbaines peuvent aider en ayant mis en place un service avec un agent mutualisé. Enfin, certains EPCI choisissent de travailler ensemble en se regroupant et en déterminant un plan d'action pour mutualiser les coûts en fonction de leurs besoins.

Question 4

Les rançongiciels (ransomware en anglais) constituent une attaque des ordinateurs via l'exécution d'un programme malveillant. Ce programme bloque l'ordinateur et réclame, pour son déblocage, le paiement d'une somme d'argent.

En cas d'infestation, il est nécessaire de débrancher le câble réseau de la machine atteinte afin de ne pas voir se propager l'infection. Il est également recommandé de ne pas éteindre l'ordinateur infecté car il serait alors plus difficile de trouver une solution palliative. Il est plutôt conseillé d'arrêter le programme via une mise en veille prolongée et de restaurer le système depuis d'anciens points de sauvegarde réalisés en amont. L'authentification de l'utilisateur doit être modifiée et l'antivirus, le pare feu doivent être analysés. Enfin, le paiement de la rançon sera prohibé, ne garantissant en aucun cas le déblocage de la machine.

Afin d'éviter les attaques de rançongiciels et de garantir la réparation des systèmes, il convient de prendre plusieurs mesures. Ces dernières, préconisées en matière de sécurité, doivent être mises au sérieux pour n'importe quelle attaque. Une formation ainsi qu'une sensibilisation des agents est requise. La mise en place d'une

charte des bonnes pratiques informatiques ainsi qu'une sécurisation des machines est nécessaire. Arrivant le plus souvent par e-mails, il faut apprendre aux agents à repérer un message électronique frauduleux notamment. Les pare feux et antivirus doivent être configurés de manière efficace sur chacun des postes. L'accès à certaines applications et lecteurs peuvent être également bloqués ou filtrés. Il est primordial d'effectuer des sauvegardes au niveau des serveurs et des applications spécifiques utilisés quotidiennement. Une sauvegarde quotidienne sur un support dématérialisé et sur un support physique déconnecté permet d'effectuer des points de restauration capitaux en cas d'attaque et de restauration des données suite à l'intrusion d'un ransomware.

Question 5.

Le shadow IT (Technologie informatique fantôme) désigne un ensemble de pratiques à risque, émanant des utilisateurs. Ces utilisateurs contournent les règles de téléchargement, ou de consultation fixées par les administrateurs. La création d'éléments par ces personnes entre également dans le shadow IT (exemple de la création d'un cloud, déplacement de matériel etc). Ce phénomène est assez peu décelable de la part des gestionnaires car chaque utilisateur peut amener une faille.

Les risques liés à ce phénomène sont présents et nombreux. La perte des données des utilisateurs en fait partie. En effet, les sauvegardes ne prennent pas obligatoirement en compte ces éléments issus des shadow IT et du travail peut être perdu. Le système d'information peut être compromis et mis à mal en cas d'utilisation d'un matériel non autorisé. La multiplication d'accès par des terminaux non recensés tels que les smartphones peut être responsable de cyber attaques en constituant des points d'attaques sensibles.