Sujet élaboré par une cellule pédagogique nationale

CONCOURS EXTERNE
TECHNICIEN TERRITORIAL

SESSION 2018

ÉPREUVE DE QUESTIONS TECHNIQUES A PARTIR D'UN DOSSIER

ÉPREUVE D'ADMISSIBILITÉ :

Réponses à des questions techniques à partir d'un dossier portant sur la spécialité au titre de laquelle le candidat concourt.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 28 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Question 1 (5 points)

Expliquez et détaillez les avantages du FttO « Fiber to the Office » par rapport au FttH « Fiber to the Home » pour répondre aux besoins des collectivités.

Question 2 (3 points)

Technicien territorial informatique, vous travaillez en collaboration avec le service aménagement du territoire. Quels sont les éléments à prendre en compte et les préconisations pour le raccordement d'une zone d'activité en très haut débit ?

Question 3 (6 points)

Vous êtes chargé par votre directeur général des services de préparer une note sur l'entrée en vigueur du règlement européen sur la protection des données :

A. Quels en sont les enjeux, notamment pour les collectivités territoriales ?

B. Quels changements vont devoir être opérés dans l'organisation de la collectivité, et comment peut-elle s'y préparer ?

Question 4 (4 points)

Quelles mesures prendre en cas d'attaque par un rançongiciel (ransomware) et comment les collectivités territoriales peuvent-elles s'en prémunir ?

Question 5 (2 points)

Qu'est ce que le « shadow IT » et quels en sont les risques ?

Liste des documents :

Document 1 : **Quelles solutions mettre en place pour une sécurité informatique accrue ?**
La Gazette des communes - Pierre Alexandre Conte - 23 Février 2017.
(3 pages)

Document 2 : **Le Très Haut Débit dans les zones d'activité. Quels enjeux, quelles perspectives ?** (Extrait).
Les notes de l'ADEUS n° 213 - Novembre 2016.
(4 pages)

Document 3 : **En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ?** (Extrait).
Commission Nationale Informatique et Libertés - Juillet 2017.
(4 pages)

Document 4 : **La sécurisation des applications comme seule réponse pour faire face au Shadow IT (Technologie informatique fantôme).**
Journaldunet.com - Serge Niango - Octobre 2017.
(2 pages)

Document 5 : **Protection contre les rançongiciels.**
Note d'information CERTFR-2017-INF-001 - Juin 2017.
(3 pages)

Document 6 : **Le shadow IT (Technologie informatique fantôme)..**
Les collectivités territoriales face à la cybercriminalité - Fiche n°8 - ANDCDG 2016.
(2 pages)

Document 7 : **5 conseils à suivre pour être en conformité avec le RGPD.**
Journal du net - Lacy Gruen - Novembre 2017.
(2 pages)

Document 8 : **Le point sur… le FttO « Fiber to the Office ».**
ant.cerema.fr - Aménagement Numérique des Territoires - 15 septembre 2017.
(5 pages)

DOCUMENT 1

Quelles solutions mettre en place pour une sécurité informatique accrue ?

La Gazette des communes - Pierre Alexandre Conte - Février 2017.

Il existe différentes méthodes permettant aux collectivités territoriales de faire face à la cybercriminalité : la formation pour éviter la faille humaine, la mutualisation pour partager savoirs et ressources, et des solutions avancées qui aident à protéger ses données.

Lorsqu'on les interroge sur la cybersécurité, nombreuses sont les collectivités territoriales qui nient encore l'importance du sujet. A l'inverse, certaines d'entre elles ont parfaitement conscience des enjeux, mais se montrent fatalistes au regard de la fréquence accrue des attaques, année après année. Pourtant, il existe de nombreuses solutions permettant de réduire nettement les risques, y compris pour les communes les plus modestes.

A travers son référentiel général de sécurité (RGS), l'Anssi a fixé un cadre réglementaire « permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens ». S'y conformer est aujourd'hui une nécessité pour les collectivités. L'agence a commencé à envoyer, à la fin de l'année 2015, un agent dans chacune des treize régions, pour gagner en proximité.

Plus simplement, un guide contenant 42 règles d'hygiène informatique a été publié le 23 janvier 2017. « Le respect d'un certain nombre de règles couvre 80 % des risques, explique Guy Flament, référent de l'Anssi dans la région Nouvelle Aquitaine. Et là, on ne parle même pas d'investissement matériel ! L'investissement va passer par la formation et la sensibilisation du personnel », ajoute-t-il.

Formation des agents publics

S'il est important de prendre en considération les failles techniques, les erreurs humaines sont extrêmement fréquentes lors d'attaques des systèmes d'information. La cybersécurité est l'affaire de tous et de chacun. Un simple clic innocent sur un lien présent dans un mail peut aujourd'hui paralyser l'ensemble des postes informatiques d'une collectivité.

Aussi, la formation revêt-elle une grande importance pour prévenir les offensives. Selon Guy Flament, il existe « un manque de sensibilisation au risque informatique » dans les collectivités. Ce dernier précise par ailleurs que la formation s'oriente souvent « vers les responsables informatiques des collectivités, qui sont déjà un peu mieux formés ».

L'accent doit donc être mis sur « la sensibilisation du personnel, de tous les personnels ». René-Yves Labranche, directeur des systèmes d'information mutualisés entre la communauté urbaine et la ville de Dunkerque, prend le problème très au sérieux : « Une fois par an, au minimum, nous lançons une information auprès des organisations syndicales lors d'un comité technique. Nous organisons également des formations sur la sécurité auprès des agents. Les nouveaux arrivants doivent valider la charte informatique et s'engager à en avoir pris connaissance. »

Mutualisation

Les collectivités locales de taille plus modeste ont tendance à se sentir démunies devant l'ampleur du problème. Elles n'ont souvent ni les moyens, ni les compétences pour faire face aux cyberattaques. « La solution, c'est la mutualisation, lance Frank Mosser, expert en cybersécurité et président de la société MGDIS. On sait aujourd'hui que pour un maire, respecter les réglementations, ça devient compliqué. Un expert en sécurité, une petite commune ne peut pas s'en payer un. »

Olivier Fouqueau est le directeur des services du syndicat intercommunal Infocom94, dans le Val-de-Marne. Celui-ci compte 19 adhérents principaux comprenant notamment des collectivités de tailles différentes, dont une commune de 2 500 habitants.

« En cumulant territoires et villes, nous couvrons environ 800 000 habitants, lance-t-il. Cela nous donne du poids dans nos relations avec les éditeurs. A la fois en termes de prix et de capacité à obtenir des mobilisations. » Avant de renchérir : « Un responsable de la sécurité des systèmes d'information (RSSI), on n'en trouve pas dans les villes petites ou moyennes. Ce sont des gens qui ont une stature, des réflexes, une vraie épaisseur en matière technique. La mutualisation nous permet d'obtenir des compétences que l'on peut se payer à plusieurs et que l'on peut partager pour faire de l'audit, des conseils, voire pour être proactif sur des problématiques de sécurité. »

Du côté de l'Anssi, Guy Flament « invite toutes les collectivités à se tourner vers les syndicats informatiques qui ont un contact privilégié avec l'agence ».

Anticipation

Faire appel à des prestataires de confiance, considérer la sécurité comme un sujet important en cas d'appel d'offres sont des mesures de bon sens. Mais parfois, l'urgence rend la prise de décision plus compliquée. Depuis plusieurs mois, les collectivités sont victimes de « rançongiciels ».

La paralysie de leur système d'information peut s'avérer extrêmement dommageable. Pour éviter de se retrouver dans une situation critique, il faut anticiper le problème et veiller à ce que ses données soient sauvegardées dans plusieurs endroits différents. Et pas uniquement dans deux salles d'un même bâtiment, par exemple.

Des plans de continuité ou de reprise d'activité permettent, dans les deux cas, le retour plus ou moins rapide à une activité normale. Pour autant, aussi frustrant soit ce constat, il faut aussi prendre conscience du fait que l'intégralité des risques informatiques ne sera jamais couverte. « Le risque zéro en matière de cybersécurité n'existe pas, conclut Guy Flament. Ou alors à des niveaux de contrainte qui ne sont pas supportables par une collectivité territoriale. L'important, c'est d'éviter l'intégralité des attaques les plus fréquentes. »

Un temps doit être consacré à la sécurité dans l'appel d'offres.
Frank Mosser, président de la société MGDIS

Par rapport aux appels d'offres auxquels on répond, la cybersécurité est un sujet que l'on met souvent en avant, mais qui n'est pas toujours mentionné au niveau de la demande, et qui n'est pas toujours un critère technique important dans le choix du prestataire. Au cours de la conception d'un logiciel, si vous enlevez le volet sécurité, cela coûte moins cher à développer. Il faut en avoir conscience. Si l'on parle d'objets connectés, de smart cities, de nouveaux services, il y a un temps qui doit être consacré à la sécurité dans l'appel d'offres. Cela doit faire partie des exigences de tout cahier des charges. Et il faut s'adjoindre les compétences pour pouvoir ensuite valider cette dimension sécuritaire.

Les 10 chapitres du guide d'hygiène informatique de l'Anssi

L'Agence nationale de la sécurité des systèmes d'information a publié un Guide d'hygiène informatique, dont les mesures « sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire ».

01 – Sensibiliser et former.
L'Agence nationale de la sécurité des systèmes d'information (Anssi) recommande de sensibiliser les utilisateurs aux bonnes pratiques en termes de sécurité informatique, mais aussi de former

les équipes opérationnelles pour éviter les erreurs générant des failles. Maîtriser les risques de l'infogérance en se posant les bonnes questions en amont est également important.

02 – Connaître le système d'information (SI).
Protéger efficacement les données sensibles nécessite de les identifier. Cela permet ensuite de localiser les postes à risque. Il faut aussi disposer d'un inventaire complet des comptes bénéficiant de droits étendus, veiller aux départs, aux arrivées et aux changements de fonctions. Enfin, les équipements qui s'y connectent doivent être maîtrisés.

03 – Authentifier et contrôler les accès.
L'Anssi incite à prêter attention au rôle de chaque personne, à attribuer les bons droits sur les ressources sensibles. Concernant l'accès au SI, les mots de passe doivent être correctement dimensionnés et, si besoin, stockés dans un endroit sécurisé. Lorsque cela est possible, l'authentification la plus forte doit être privilégiée.

04 – Sécuriser les postes.
Cette mesure implique de mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique, de configurer un pare-feu avec précaution, de chiffrer les données sensibles transmises par internet, de proscrire l'utilisation de supports amovibles tels que les clés USB et d'homogénéiser les politiques de sécurité.

05 – Sécuriser le réseau.
Outre le fait de protéger l'accès physique aux serveurs et aux locaux techniques, l'Anssi recommande de veiller à segmenter et à cloisonner le réseau pour éviter que toutes les machines soient liées entre elles. Utiliser des protocoles réseaux sécurisés, protéger la messagerie professionnelle, font partie des autres conseils.

06 – Sécuriser l'administration.
La navigation sur internet comporte de nombreux risques. Il convient donc d'interdire l'accès au web depuis les postes ou serveurs utilisés pour l'administration du SI. L'utilisation d'un réseau dédié et cloisonné est encouragée. Par ailleurs, il faut limiter au strict besoin opérationnel les droits d'administration.

07 – Gérer le nomadisme.
Il faut prendre des mesures de sécurisation physique, mais aussi chiffrer les données sensibles en cas de perte du matériel nomade. S'assurer de la sécurisation de la connexion de l'appareil au réseau du SI est aussi crucial. Plus globalement, adopter des politiques de sécurité dédiées aux terminaux mobiles apparaît indispensable.

08 – Maintenir le système d'information à jour.
Les failles contenues dans les logiciels sont particulièrement dangereuses. Mais elles sont progressivement corrigées. Aussi, il est important de s'équiper des versions les plus récentes des différents outils pour minimiser les risques. Anticiper la fin de leur maintenance est également essentiel.

09 – Superviser, auditer, réagir.
L'Anssi préconise, si possible, de désigner un RSSI, mais aussi de procéder régulièrement à des contrôles et audits de sécurité. Il convient également de mettre en place une politique de sauvegarde des composants critiques. En cas d'incident, disposer d'une procédure de gestion s'avère essentiel pour éviter de commettre des erreurs.

10 – Privilégier l'usage des produits et services qualifiés par l'Anssi.
L'agence propose une liste de produits et de prestataires qualifiés par ses soins. Elle encourage l'utilisation de ces derniers pour toute entité, car elle estime qu'il s'agit du seul gage d'une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème.

DOCUMENT 2

LeTrès Haut Débit dans les zones d'activité. Quels enjeux, quelles perspectives ? (Extrait).

Les notes de l'ADEUS n° 213 - Novembre 2016.

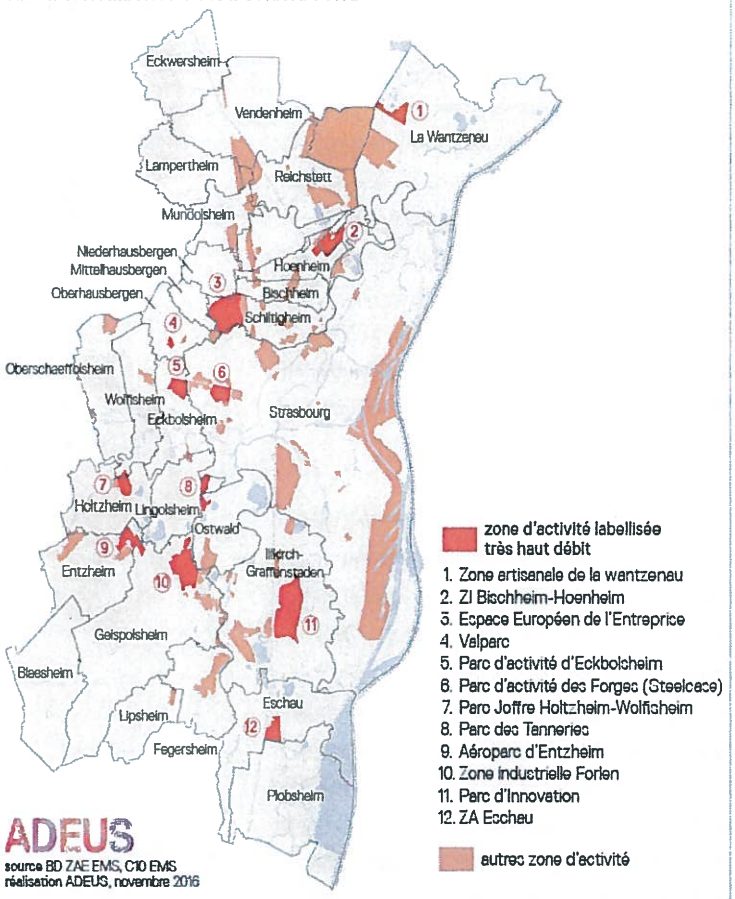
Desserte en très haut débit des zones d'activités

Où ?

L'Eurométropole de Strasbourg compte 12 zones d'activité « ZA THD ». Ce label créé en 2011 a pour objectif de soutenir l'équipement en très haut débit des zones d'activité en stimulant l'offre par le pré-équipement en infrastructures numériques et en donnant de la visibilité sur l'accessibilité en très haut débit aux entreprises souhaitant s'implanter. Il distingue ainsi 115 zones d'activité en France disposant de conditions favorables à la présence d'une offre très haut débit. Il reste cependant difficile d'identifier les zones qui disposent réellement du très haut débit. L'obtention du label ne signifie pas que l'ensemble des entreprises présentes dans la zone sont effectivement desservies par la fibre optique. Même si la zone est potentiellement fibrée, les entreprises ne sont souvent pas prêtes à investir la somme nécessaire pour être raccordées. A l'inverse, certaines zones peuvent disposer du très haut débit sans être identifiées par le label. L'ancienne Direction générale des entreprises (DGCIS) a interrompu la démarche de labellisation des zones d'activité en novembre 2013. Le projet de loi pour une République numérique prévoit désormais la création d'un statut de « zone fibrée » pour les territoires desservis par un réseau à très haut débit en fibre optique FttH permettant d'assurer la transition complète du réseau cuivre.

Le raccordement effectif des entreprises au THD dépend à la fois de la nature de leur activité et de leur taille. Plus la taille de l'entreprise augmente, plus elle augmente ses besoins en débit et donc en bande passante. Elle est également davantage susceptible de s'organiser sur plusieurs sites, nécessitant un échange entre ces derniers. Les entreprises de plus de 1 000 salariés sont ainsi généralement fibrées. L'activité de l'entreprise et ses usages numériques sont également un critère déterminant pour l'obtention du THD. A noter que toutes les entreprises sont amenées à s'intéresser au débit dont elles disposent, le débit nécessaire pour leurs activités étant en moyenne triplé tous les trois ans en raison du volume de données envoyées et réceptionnées. Beaucoup de PME gardent cependant une vision grand public des télécommunications et comprennent difficilement le montant des frais de raccordement et le coût des forfaits que leur proposent les opérateurs.

LABELLISATION ZONE D'ACTIVITÉ TRÈS HAUT DÉBIT DANS L'EUROMÉTROPOLE DE STRASBOURG



CRITÈRES À RESPECTER POUR UNE OFFRE ÉQUIVALENTE À CELLE DES ZONES D'ACTIVITÉ LABELLISÉES

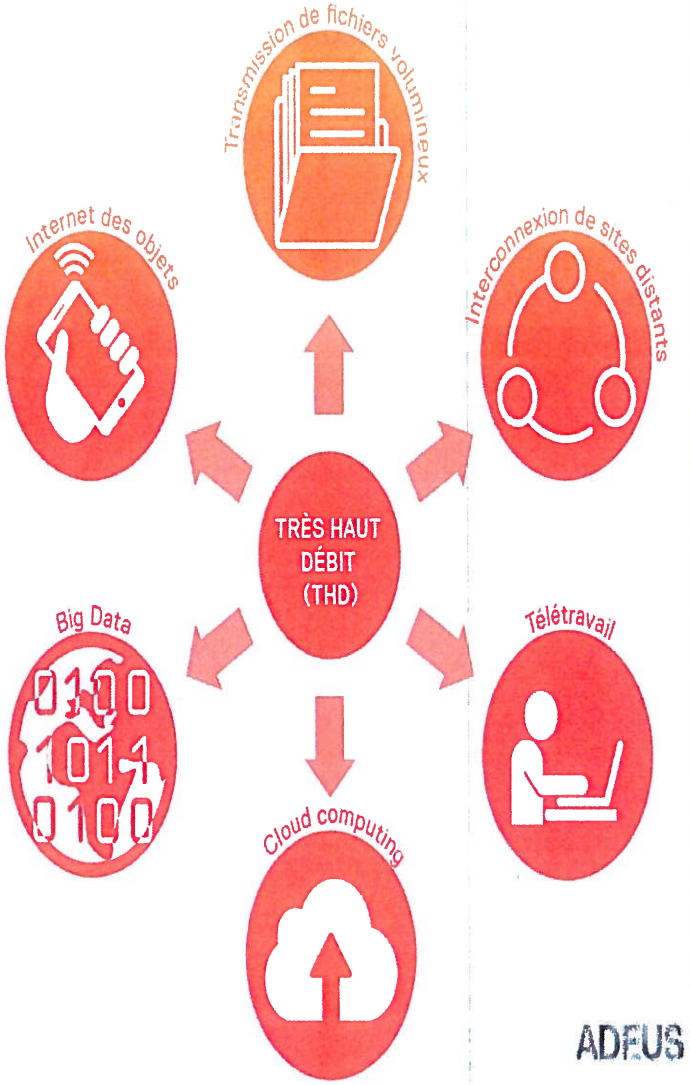
1. Chaque entreprise peut être raccordée au très haut débit grâce :
   - au raccordement en fibre optique à au moins un réseau de collecte en entrée de zone,
   - à l'engagement de l'opérateur à offrir des liaisons THD aux entreprises,
   - à la présence proche de chaque parcelle de points d'adduction du réseau de télécommunications.
2. La concurrence est effective : les entreprises peuvent choisir entre plusieurs opérateurs, au moins deux, qui s'engagent à leur répondre dans un délai de trois mois.
3. La zone d'activité est équipée en infrastructures d'accueil (les fourreaux dans lesquels les câbles optiques sont insérés, les chambres donnant accès à ces conduites et les locaux techniques hébergeant les équipements actifs de l'opérateur) permettant l'accueil de la fibre optique et la mise en concurrence entre opérateurs. La présence des infrastructures d'accueil requises suffit pour répondre aux critères du label.

Pourquoi ?

La desserte en THD des zones d'activité soulève des enjeux de développement économique par ses impacts sur l'attractivité, la compétitivité et la création de valeur ajoutée pour le territoire comme pour ses entreprises. La transition numérique de l'ensemble des entreprises est en cours de réalisation. Chaque filière d'activité est concernée par un bouquet de services numériques défini par le gouvernement dans le cadre de sa stratégie numérique. L'évolution des usines vers l'industrie du futur et le recours croissant aux bases de données dans l'ensemble des secteurs d'activité fait par ailleurs courir le risque aux PME d'être exclues des réseaux de sous-traitance si elles ne disposent pas d'une desserte numérique satisfaisante. Le THD valorise les zones d'activité. Il permet une meilleure commercialisation des locaux et le maintien des entreprises locataires dans la zone.

Les entreprises éprouvent souvent des difficultés à cerner et à exprimer leurs besoins réels en matière de THD. Pour faciliter cet autodiagnostic, l'Eurométropole de Strasbourg propose un outil permettant de cibler et d'expliciter les besoins individuels de chaque entreprise, ainsi qu'un guide explicatif des offres proposées par les opérateurs. La CCI Alsace sensibilise par ailleurs les entreprises aux enjeux du THD tels que la nécessité de s'adapter aux services et usages émergents ou déjà actuels. L'utilisation d'outils collaboratifs ou le travail multi-sites en flux continu nécessitent par exemple des débits plus importants et symétriques, ainsi qu'un faible temps de latence. Les entreprises ont également besoin d'une garantie de rétablissement rapide en cas de dysfonctionnement et d'un raccordement sécurisé. Deux niveaux de sécurisation peuvent être distingués. Dans le premier cas, la fibre optique utilisée pour relier l'entreprise à Internet est doublée par un deuxième cheminement partant du même central. Dans le second cas, l'entreprise dispose d'un central de secours afin de pallier au risque de panne du premier. Le deuxième cheminement de secours peut par ailleurs utiliser une autre technologie.

SERVICES ET USAGES NÉCESSITANT LE TRÈS HAUT DÉBIT



Source : ADEUS

Comment ?

Les offres des opérateurs dépendent du destinataire et de la technologie utilisée. L'offre xDSL (Digital Suscriber Line ou ligne numérique d'abonné) s'appuie sur un support cuivre. L'ADSL propose un débit asymétrique, le SDSL un débit symétrique et le VDSL le très haut débit mais seulement sur de courtes distances. L'offre destinée aux zones d'activité est la fibre FttO (Fiber to the office). L'entreprise dispose d'un lien en fibre optique dédié et des débits symétriques garantis par l'opérateur, contrairement à la fibre FttH (Fiber to the Home). L'offre FttO s'accompagne de services tels que la sécurisation de la ligne et la garantie de son rétablissement dans un délai de quatre heures. Dans l'offre FttH proposée aux particuliers, le débit est asymétrique et non garanti car le lien en fibre optique est mutualisé et partagé entre les utilisateurs. La différence de prix entre l'offre FttO professionnelle et celle FttH résidentielle s'explique par la différence de raccordement et les services complémentaires associés au FttO.

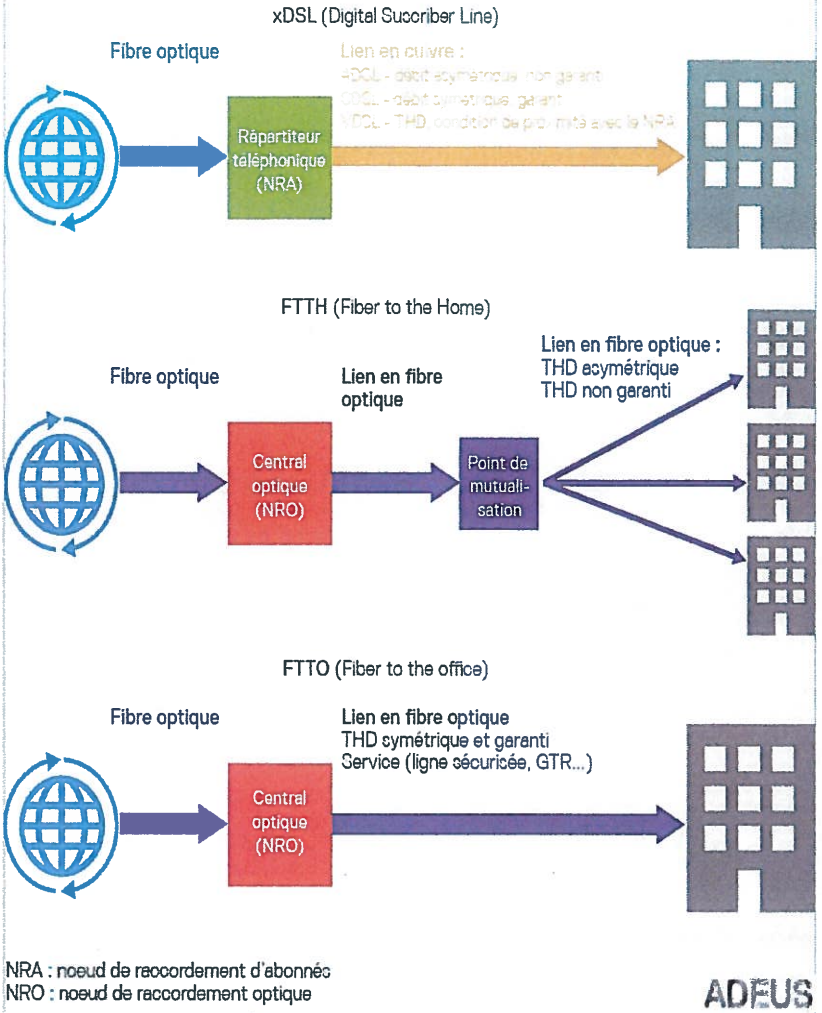
Pour qu'une zone d'activité puisse être desservie en THD, elle doit être équipée d'infrastructures d'accueil permettant le passage de la fibre optique jusqu'à chaque parcelle. L'aménageur doit prévoir la mise en place au sein de la zone :

- d'une chambre technique d'adduction par parcelle, implantée sur le domaine public, qui permet le raccordement au réseau de fourreaux de la zone ;
- des fourreaux qui relient les chambres d'adduction à la chambre de tirage à l'entrée de la zone.

L'aménageur doit également assurer l'interface entre le réseau de collecte de l'opérateur et le réseau de desserte de la zone avec :

- une chambre de raccordement mutualisée à l'entrée de la zone ou des chambres individuelles pour chaque opérateur à partir desquelles la fibre est dérivée du réseau de collecte afin de raccorder la zone ;
- un local technique à l'entrée de la zone et à proximité immédiate de la chambre de tirage, permettant aux opérateurs d'héberger leurs équipements ;
- une nappe de fourreaux reliant la/les chambre(s) de raccordement et le local technique à l'entrée de la zone ;
- une chambre de tirage mutualisée et à proximité immédiate du local technique, par laquelle passent toutes les fibres qui irriguent la zone d'activité.

TROIS TYPES DE RACCORDEMENT POUR ACCÉDER AU TRÈS HAUT DÉBIT

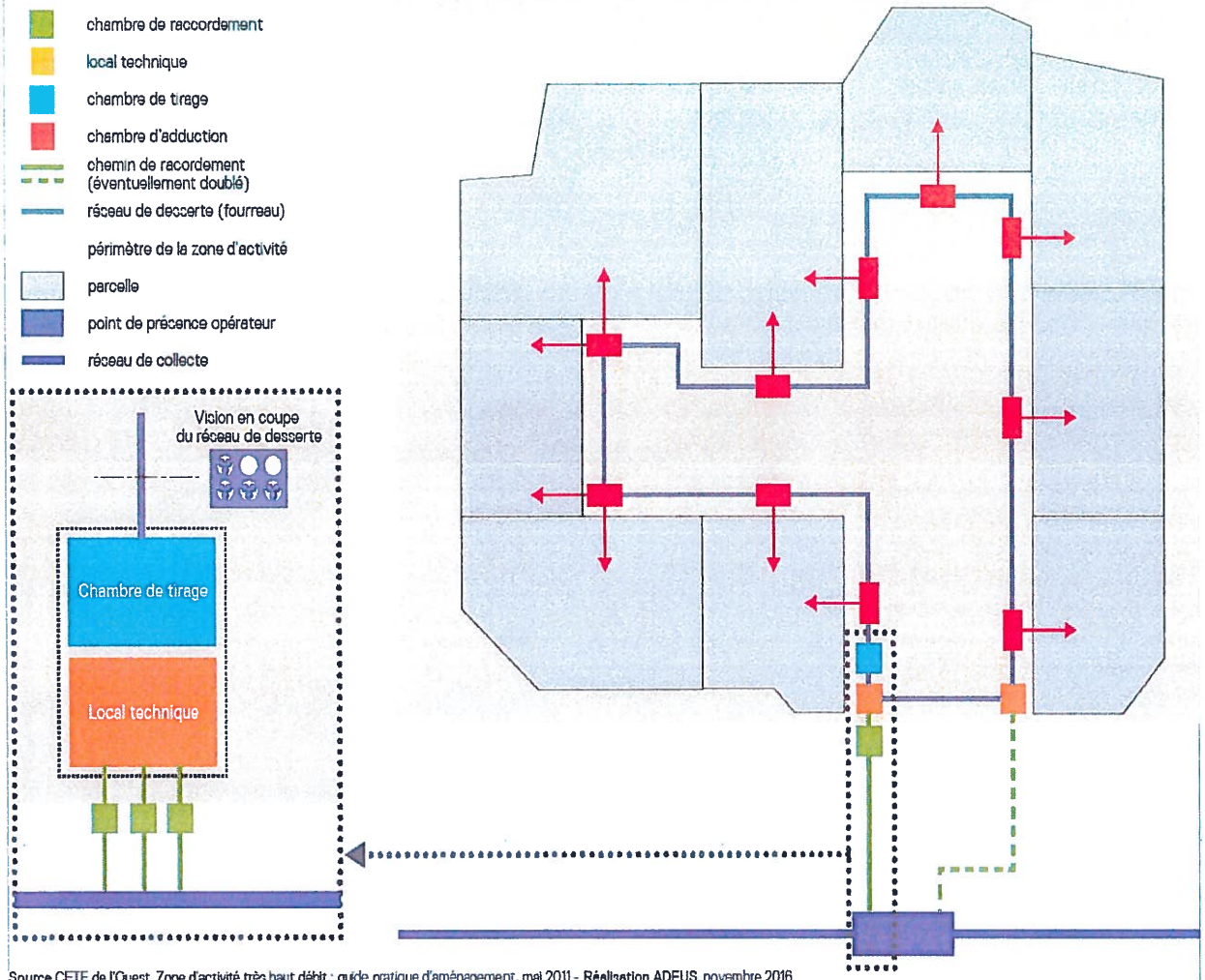


NRA : noeud de raccordement d'abonnés
NRO : noeud de raccordement optique

Source : Alfa-Safety - Réalisation : ADEUS

ADEUS

INFRASTRUCTURES D'ACCUEIL NÉCESSAIRES À LA DESSERTE EN THD D'UNE ZONE D'ACTIVITÉ



Source CETE de l'Ouest, Zone d'activité très haut débit : guide pratique d'aménagement, mai 2011 - Réalisation ADEUS, novembre 2016

Dans le cas d'une zone d'activité existante, il convient de commencer par le recensement des infrastructures d'accueil existantes. Cet état des lieux s'appuie sur les documents existants (plans de récolement, conventions d'occupation ou encore délibérations de conseils municipaux) et un relevé sur site. Le recensement ne se limite pas aux seules infrastructures de télécommunications. Il importe de connaître également l'existence et la disponibilité de réseaux tiers, capables d'accueillir des câbles optiques, telles que les canalisations de gaz abandonnées, d'assainissement, d'électricité ou encore d'éclairage public. Une fois les informations sur le patrimoine existant saisies dans un logiciel SIG, il s'agit de l'adapter s'il s'avère insuffisant en complétant le manque de fourreaux, de chambres et de locaux techniques. Les fourreaux doivent permettre d'assurer un chemin vide continu pour plusieurs opérateurs entre chaque parcelle et le point d'entrée de la zone d'activité. La mise à niveau peut alors passer par l'augmentation du nombre de fourreaux, leur sous-tubage ou l'optimisation des infrastructures existantes en demandant par exemple aux opérateurs de retirer les câbles non utilisés ou en utilisant les réseaux tiers.

Dans le cas de création d'une nouvelle zone d'activité, les infrastructures d'accueil sont intégrées dans le programme des travaux. La pose des fourreaux et la mise en place des chambres s'effectuent lors de la viabilisation de la zone, en même temps que les autres réseaux secs (gaz et électricité). S'ils ne sont pas réalisés avant la livraison des bâtiments, l'aménageur doit réserver des emplacements pour la construction des locaux techniques. Les entreprises devront ensuite prendre contact avec les opérateurs.

L'aménageur peut aller au-delà de la seule mise en place des infrastructures d'accueil et décider de déployer de la fibre noire, c'est-à-dire des câbles optiques non activés qu'il louera aux opérateurs. Il lui faudra néanmoins veiller à ce que son architecture optique soit compatible avec les choix technologiques des opérateurs. Elle ne garantit néanmoins pas la venue de ces derniers. La mise en relation avec un opérateur reste impérative. Sans connexion au réseau Internet de ce dernier, l'échange d'informations et de données ne sera possible qu'entre entités de la zone fibrée.

DOCUMENT 3

En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ? (Extrait).

Commission Nationale Informatique et Libertés - Juillet 2017.

Les collectivités territoriales traitent chaque jour de nombreuses données personnelles, que ce soit pour assurer la gestion administrative de leur structure (fichiers de ressources humaines), la sécurisation de leurs locaux (contrôle d'accès par badge, vidéosurveillance) ou la gestion des différents services publics et activités dont elles ont la charge.

Certains de ces traitements présentent une sensibilité particulière, comme les fichiers d'aide sociale et ceux de la police municipale.

Quels sont les enjeux des collectivités en matière de protection des données ?

Le développement de **l'e-administration** constitue un levier majeur de la modernisation de l'action publique. De ce fait, les collectivités recourent de plus en plus aux technologies et usages numériques : téléservices, open data, systèmes d'information géographique, *Cloud computing*, compteurs intelligents, réseaux sociaux, lecture automatique de plaques d'immatriculation, etc.

Par ailleurs, le nombre de **cyber attaques** ne cesse d'augmenter, et ce, quel que soit la taille des organisations visées.

De plus, **les citoyens sont de plus en plus soucieux** de la manière dont leurs données sont utilisées. A ce titre, la loi pour une République numérique est venue consacrer en octobre 2016 un droit à l'auto-détermination informationnelle que l'on retrouve posé à l'article 1er de la loi Informatique et Libertés : « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant* ».

Les nouveaux services numériques, pour qu'ils créent de la confiance auprès des administrés, doivent donc répondre aux exigences de protection des données dont **la sécurité** est une des composantes essentielles.

Enfin, la nécessité pour les collectivités de prendre en compte ces exigences est aujourd'hui d'autant plus importante que le règlement européen sur la protection des données, applicable à compter du 25 mai 2018, renforce encore les obligations en matière de transparence des traitements et de respect des droits des personnes, s'axe sur une logique globale de responsabilisation de l'ensemble des acteurs et crédibilise la régulation des « CNIL » en musclant considérablement leur pouvoir de sanction. Ainsi, outre des avertissements publics, elles pourront prononcer des amendes administratives allant jusqu'à 20 millions d'euros ou, pour une entreprise, 4% du chiffre d'affaires mondial.

En quoi le règlement européen sur la protection des données impacte-t-il les collectivités territoriales ?

Une logique de responsabilisation

Si les grands principes déjà présents dans la loi Informatique et Libertés ne changent pas, **un véritable changement de culture s'opère**. On passe en effet d'une logique de contrôle a priori basé sur des formalités administratives à une **logique de responsabilisation** des acteurs privés et publics. Ce changement de posture devra se traduire par **une mise en conformité permanente et dynamique de la part des collectivités. Elles devront ainsi adopter et actualiser des mesures techniques et organisationnelles leur permettant de s'assurer et de démontrer à tout instant qu'elles offrent un niveau optimal de protection aux données traitées.**

Les organismes publics et privés auxquels les collectivités sous-traitent la mise en œuvre de tout ou partie de leurs traitements (ex. : prestataires de service hébergeant des données) devront

obligatoirement participer à la démarche de mise en conformité, en aidant celles-ci à satisfaire leurs diverses obligations, sous peine de sanctions.

La protection des données dès la conception et par défaut

Les collectivités devront intégrer un nouveau principe de protection des données dès la conception (Privacy by design) du traitement et par défaut (Privacy by default).

Elles devront ainsi tenir compte le plus en amont possible, dès la phase de conception du produit, du service ou du traitement, de définition des outils qui seront utilisés et des paramétrages par défaut, des règles d'or de la protection des données. Il s'agira en particulier de minimiser à tout point de vue le traitement effectué.

Par exemple :

- *favoriser par principe les menus déroulants ou les cases à cocher plutôt que les zones de commentaires libres sur les formulaires de collecte et dans les bases de données internes, pour limiter dès le départ le nombre et la nature des données enregistrées* ;
- *restreindre au maximum les droits d'accès informatiques aux données et les opérations susceptibles d'être réalisées ;*
- *pseudonymiser les données toutes les fois où leur exploitation sous une forme identifiante n'apparaît pas nécessaire à la satisfaction du besoin ;*
- *appliquer un mécanisme automatique de purge des données à l'issue de la durée de conservation nécessaire à la réalisation de la finalité.*

La gouvernance des données

Avec le règlement, on assiste à un allègement considérable des obligations en matière de formalités préalables, puisque le régime déclaratif est totalement supprimé, pour rentrer dans l'ère de la gouvernance des données personnelles. Une bonne gouvernance nécessite toutefois une documentation continue des actions menées pour être en capacité de piloter et de démontrer la conformité. Les collectivités seront ainsi appelées à tenir un registre de leurs activités de traitement, à encadrer les opérations sous-traitées dans les contrats de prestation de services, à formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des demandes d'exercice des droits, à adhérer à des codes de conduite ou encore à certifier des traitements.

Dans certains cas, pour les traitements à risques, elles devront effectuer des analyses d'impact sur la vie privée et notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles.

La désignation d'un délégué à la protection des données est-elle obligatoire pour les collectivités ?

A compter du 25 mai 2018, la désignation d'un délégué à la protection des données (*Data protection Officer*), successeur du correspondant informatique et libertés (CIL) dont la désignation est aujourd'hui facultative, sera obligatoire pour les organismes et autorités publics, et donc pour les collectivités.

Missions

Le délégué aura **pour principales missions** :

- d'informer et de conseiller le responsable de traitement de la collectivité ou le sous-traitant, ainsi que les agents ;
- de diffuser une culture Informatique & Libertés au sein de la collectivité ;
- de contrôler le respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier ;

- de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec la CNIL et d'être le point de contact de celle-ci.

Dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.

Expertise et moyens

De plus, la collectivité devra s'assurer qu'il dispose **d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace**. Ainsi, le délégué devra :

- être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ;
- être associé en temps utile et de manière appropriée à l'ensemble des questions Informatique & Libertés ;
- bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

Dans ce contexte, la mutualisation de la fonction de DPO apparaît un enjeu essentiel pour les collectivités territoriales, notamment pour celles de petite taille.

A quel niveau envisager la mutualisation du délégué à la protection des données ?

Aujourd'hui, si les grandes collectivités ont déjà engagé cette démarche (2/3 des régions, la moitié des départements, 2/3 des métropoles, 1/3 des communautés urbaines, 1/10 des communautés d'agglomération), seulement 2% des communes ont désigné un correspondant.
Pour ces collectivités, qui ont des préoccupations identiques, la mutualisation de la fonction semble tout à fait adaptée. Elle permet de limiter les coûts et de bénéficier de professionnels disposant des compétences et de la disponibilité nécessaires à un bon pilotage de la conformité.

Les structures de mutualisation informatique (SMI) et les centres de gestion

Les structures de mutualisation informatique, spécialisées dans le développement de l'e-administration sur leur territoire, constituent une bonne solution de mutualisation de la fonction de délégué pour les collectivités. Ces structures portent très souvent le développement numérique des territoires, que ce soit à travers le réseau des infrastructures ou des services proposés (ex. : plateformes de téléservices), et proposent aux collectivités un accompagnement dans leur transition numérique.

Elles regroupent maîtrise d'ouvrage et maîtrise d'œuvre et c'est à leur niveau que les besoins des collectivités sont identifiés, que des progiciels sont développés, que les mesures de sécurité et paramétrages par défaut sont définis, et qu'éventuellement les données sont hébergées. Ayant vocation à se multiplier, elles couvrent déjà 50% des départements et permettent aux collectivités adhérentes de rationaliser les dépenses tout en optimisant les conditions juridiques, organisationnelles et fonctionnelles du déploiement d'outils numériques de gestion de leurs missions de service public.

Certaines de ces structures, telles que l'ALPI (Agence landaise pour l'informatique) propose déjà un service de CIL mutualisé aux communes, établissements publics et groupements de collectivités de leur ressort territorial. D'autres, telles que l'ADICO dans l'Oise (association pour le développement et l'innovation numérique des collectivités) ont commencé à travailler sur une offre de délégué mutualisé.

A noter aussi que des collectivités bénéficient dès à présent de CIL mutualisés au niveau de centres de gestion de la fonction publique territoriale (CDG11, CDG54, CDG60 et le CDG59).

Les établissements publics de coopération intercommunale (EPCI)

Les communautés de communes, d'agglomération, les communautés urbaines et les métropoles, peuvent également proposer aux collectivités qui en sont membres les services d'un délégué mutualisé.

Enfin, sans aller jusqu'à mutualiser la fonction de délégué, les collectivités ayant les mêmes préoccupations peuvent opportunément travailler ensemble pour se préparer au mieux aux nouvelles obligations posées par le règlement européen. Les 12 départements de la région Nouvelle Aquitaine se sont ainsi engagés dans une telle démarche : identification des besoins des uns et des autres, définition d'un plan d'action comprenant différentes étapes, développement d'un outil commun d'information et de partage de connaissances, etc.

DOCUMENT 4

La sécurisation des applications comme seule réponse pour faire face au Shadow IT (Technologie informatique fantôme).

Journaldunet.com - Serge Niango - Octobre 2017.

Trop souvent, les utilisateurs les plus productifs font l'acquisition d'applications non approuvées sans en informer les services IT. Or, ils ne sont peut-être pas conscients des risques qu'impliquent ces applications non validées

Depuis les toutes dernières applications pour smartphone aux plus récents assistants vocaux, chacun a su faire place à l'innovation dans son quotidien. Et il serait bien dommage de s'en priver. Après tout, ces avancées technologiques améliorent notre vie, nous rendent plus productif et performant et nous aident à rester connectés. Voilà pourquoi, aujourd'hui nous sommes nombreux à faire du smartphone un élément essentiel de notre travail et à nous ruer sur chaque nouvelle application, nouveau service susceptible de nous faciliter la tâche.

Shadow IT, un risque pour les entreprises

Si parfois les services IT n'évoluent pas aussi vite que le voudraient les employées, il n'est pas si compliqué de contourner la procédure classique pour télécharger une application ou s'inscrire à un service cloud sans en informer l'IT. Mais trop souvent, les utilisateurs les plus productifs et les plus ambitieux font l'acquisition d'applications et de technologies non approuvées sans en informer les services informatiques – ce que l'on appelle communément le Shadow IT. Or, ces derniers ne sont peut-être pas conscients des risques qu'impliquent ces applications non validées, qui peuvent, in fine, mettre en danger leurs données personnelles et leur entreprise.

Cette tendance du Shadow IT peut exposer les entreprises à l'exfiltration de données, des malwares ou encore des tentatives de phishing. Plus grave encore, elle peut ouvrir la voie au vol de l'identité de collaborateurs, de clients, ou de secrets de fabrication. Et pire encore, conduire les entreprises à ne pas se satisfaire aux règles en vigueur et à enfreindre la loi. Et de fait, le Shadow IT étant causé par des utilisateurs peu précautionneux et imprévisible, il est difficile pour les services IT de prévenir, gérer et contrôler.

Privilégier un environnement de travail unifié

Dans ces conditions, comment les entreprises peuvent-elles fournir à leurs employés les applications et outils qu'ils souhaitent, sur les équipements de leur choix, sans pour autant compromettre la sécurité ? Un environnement de travail unifié et sécurisé peut déjà être un premier élément de réponse. En proposant des outils, applications et services efficaces, complets et en adéquation avec leurs attentes, les salariés seront moins enclins à recourir au Shadow IT, de sorte que l'IT pourra reprendre la main et limiter les dégâts.

Avec un environnement de travail unifié, le quotidien de l'utilisateur est grandement simplifié avec une identification unique et de manière sécurisée, lui permettant de vaquer à ses tâches, et ce dans un seul et même environnement numérique. Non seulement cela lui évite d'avoir à se connecter de multiple fois à de multiples applications (SaaS, entreprises...) et autres services web. Mais cela rend aussi moins tentante l'utilisation d'applications et de services non approuvés. Une simplification du travail et des process peut garantir une meilleure reconnaissance des salariés pour les applications fournies par l'entreprise.

Et en même temps, un environnement de travail unifié facilite également le quotidien des équipes IT. Les administrateurs peuvent gérer l'ensemble comme un service unique et y ajouter sans difficulté des applications, services et capacités supplémentaires à la demande. Ainsi, les services IT et sécurité gagnent en agilité et en réactivité, au bénéfice de tous les utilisateurs.

En outre, il importe que toutes les applications et tâches, dans le cadre de cet environnement de travail unifié et sécurisé, soient managées à partir du cloud, de sorte que les administrateurs

puissent assurer le suivi, la maintenance et la gestion des workloads exécutées sur site et dans le cloud, y compris des services provenant de clouds multiples, en un seul et même lieu. Ce modèle facilite considérablement l'administration des environnements hybrides, il est plus économique, et l'entreprise peut adapter la capacité des services cloud à ses besoins opérationnels.

Ne pas faire l'impasse sur la sécurité

La sécurité est une condition sine qua non pour tout environnement de travail unifié. Les services de virtualisation permettent de sécuriser le déploiement des applications et des données, en les conservant hors des équipements. Pour les applications mobiles, le service de mobilité offre une gestion sécurisée des appareils et des applications, notamment en maintenant les données dans un environnement chiffré.

Par ailleurs, il est essentiel de contextualiser la sécurité afin qu'elle puisse adapter ses paramètres et ceux des applications au réseau, à l'équipement et au lieu de travail de l'utilisateur. Par exemple, un collaborateur se rendant chez un client dans un pays jugé à haut risque pourra se voir imposer d'utiliser une carte à puce virtuelle pour avoir accès au réseau de l'entreprise. Par contre, le collaborateur n'aura pas à satisfaire à cette obligation lorsqu'il accède aux mêmes applications et données depuis le siège de l'entreprise. L'environnement de travail numérique sécurisé fonctionne selon un modèle d'accès contextuel afin de garantir la protection des applications et des données à chaque stade de leur utilisation.

Les utilisateurs attendent aujourd'hui d'une technologie, qu'elle soit simple, pratique et facile à utiliser. En déployant un environnement de travail unifié et sécurisé, les entreprises peuvent simplifier leur travail et leur permettre d'utiliser librement leurs équipements favoris, tout en réduisant la tentation du Shadow IT et les risques liés à des technologies non approuvées. Ainsi, collaborateurs comme dirigeants seront satisfaits, et l'entreprise plus sécurisée.

DOCUMENT 5

Protection contre les rançongiciels.

Note d'information CERTFR-2017-INF-001 - Juin 2017.

1 – Les rançongiciels

Les rançongiciels (ransomware en anglais) constituent une catégorie de programmes malveillants visant à obtenir le paiement d'une rançon. Pour ce faire, le programme malveillant essaie le plus souvent d'empêcher l'utilisateur d'accéder à ses fichiers, par exemple en les chiffrant, et lui affiche des instructions afin que celui-ci paie une rançon.

Lorsqu'un ordinateur est infecté, les fichiers de cet ordinateur peuvent être bloqués, mais les conséquences peuvent aussi s'étendre au reste du système d'information. Ainsi, un partage de fichiers monté sur une seule machine infectée se retrouvera probablement concerné et risque ainsi d'impacter un plus grand nombre d'utilisateurs. De même, si l'infection initiale arrive souvent (mais pas nécessairement) par un courrier électronique piégé, le programme peut aussi chercher à se propager de manière autonome sur le reste du système d'information et au travers de ses interconnexions en exploitant des vulnérabilités à distance. Si certains de ces programmes comportent des défauts de fabrication permettant de retrouver partiellement ou totalement les données concernées, d'autres utilisent des méthodes proches de l'état de l'art et peuvent condamner l'accès aux fichiers si la clé de déchiffrement n'est pas obtenue. Il s'agit donc effectivement d'une menace à prendre très au sérieux et dont il vaut mieux chercher à se prémunir avant qu'il ne soit trop tard.

2 – Prévention

Assurer un bon niveau de sécurité globale du système d'information

Pour infecter de manière automatisée une machine, un rançongiciel doit utiliser une vulnérabilité (ex : macro malveillante dans un document piégé, vulnérabilité logicielle d'un service réseau, mot de passe par défaut, etc.). Ainsi, afin de réduire les possibilités offertes à un rançongiciel de s'introduire, il convient d'assurer un bon niveau de sécurité global du système d'information.

Si l'objectif de ce document n'est pas de constituer un guide de sécurisation d'un système d'information, quelques bonnes pratiques sont par exemple référencées dans le guide d'hygiène de l'ANSSI. Parmi les mesures s'appliquant particulièrement dans le cadre de ce document, on peut citer :

- appliquer les correctifs de sécurité fournis par les éditeurs ;
- restreindre les programmes autorisés à être exécutés : application de stratégies de restriction logicielle ou de Applocker pour les systèmes Windows, options de montage en lecture seule des répertoires temporaires et de l'utilisateur pour les systèmes UNIX ;
- durcir la configuration des logiciels bureautiques ou manipulant des données provenant d'Internet : restreindre l'autorisation des macros dans les suites bureautiques, désactiver le moteur JavaScript des lecteurs PDF, activer les bacs à sable (sandbox) des logiciels le permettant, installer des extensions dédiées aux navigateurs Internet pour restreindre par défaut l'interprétation de code JavaScript, etc. ;
- configurer le pare-feu des postes de travail pour empêcher les flux de poste à poste ;
- lorsque des anti-virus sont employés sur les postes ou sur les passerelles de messagerie, veiller à la mise à jour fréquente des signatures et du moteur du logiciel ;
- minimiser les droits sur les partages réseau : s'assurer que le droit en écriture n'est accordé qu'aux utilisateurs en ayant réellement le besoin et contrôler régulièrement les droits d'accès ;
- effectuer des sauvegardes et des tests de restauration. Procéder à la mise hors ligne des sauvegardes des éléments les plus sensibles. Ces points sont développés par la suite ;
- effectuer des audits et des tests d'intrusion réguliers et mettre en place un plan d'action pour corriger les défauts mis en évidence.

Sensibiliser les utilisateurs

Si le rançongiciel n'affecte pas de manière automatisée une machine, le vecteur d'infection sera l'utilisateur, que ce soit à son insu en ouvrant une pièce jointe piégée ou par inadvertance en désactivant une protection (technique d'ingénierie sociale incitant l'utilisateur à effectuer une action).

La sensibilisation des utilisateurs est ainsi primordiale :

- ne pas ouvrir les pièces jointes des messages électroniques suspects (fautes d'orthographes, pièces jointes au nom trop succinct ou trop générique, etc.). Il faut toutefois noter que la caractéristique d'un courriel de type « hameçonnage ciblé » (spear phishing) est de personnaliser le contenu par rapport à l'environnement de l'utilisateur afin de duper sa vigilance ;
- ne pas suivre les liens des messages électroniques suspects et vérifier la cohérence entre l'adresse affichée dans le contenu et le lien effectif. Il faut toutefois noter que les attaques de type XSS (cross-site scripting) ou par point d'eau (watering hole) rendent inefficace cette pratique ;
- ne pas réactiver des fonctionnalités désactivées dans la configuration des logiciels, même si le fichier ouvert y incite par un message particulier.

Effectuer des sauvegardes

La charge malveillante des rançongiciels étant de chiffrer des fichiers, la principale mesure permettant d'éviter les pires conséquences consiste à réaliser des sauvegardes, en priorité des serveurs de fichiers et des applications métier critiques. Il convient de garder à l'esprit que ces sauvegardes peuvent aussi, intentionnellement ou non, être victimes d'un rançongiciel. Il convient donc de les protéger de manière adéquate. Le moyen, souvent le plus sûr, mais aussi le plus simple, consiste à stocker une copie de ces sauvegardes sur un support déconnecté. Dans de nombreux cas, de simples disques durs amovibles peuvent suffire. Sur un périmètre large, cette méthode peut être privilégiée pour les données les plus sensibles. Des tests de restauration des sauvegardes doivent être régulièrement effectués afin de s'assurer que la procédure soit connue et que les sauvegardes soient complètes et intègres. Par ailleurs, pour des besoins particuliers, notamment en environnement industriel, s'assurer de la disponibilité d'équipements de secours dont les configurations sont sauvegardées hors ligne est primordial. De même, la possibilité de remplacer immédiatement un poste de commande doit être établie (image disque, équipements de spare à froid, poste ou chaine dupliquée hors ligne, etc.).

3 – En cas d'infection

Débrancher la machine du réseau informatique

Afin d'arrêter la propagation de l'infection hors de la machine victime, il convient de l'isoler du réseau en débranchant le câble réseau. Il est également nécessaire de vérifier si une éventuelle connexion sans fil (Wi-Fi) est présente et, le cas échéant, de la désactiver, de préférence avec l'interrupteur matériel.

Ne pas éteindre la machine concernée

Il est parfois possible de retrouver en mémoire des éléments permettant de recouvrer les fichiers victimes. Cependant, l'extinction d'une machine ou l'ancienneté d'une infection peuvent réduire les chances de fonctionnement d'une éventuelle méthode de recouvrement. Si la machine le permet, il est recommandé d'activer la mise en veille prolongée, afin d'arrêter l'activité du programme malveillant tout en préservant la mémoire pour une analyse ultérieure. Parallèlement, au cas où le processus de chiffrement n'aurait pas été terminé, les fichiers peuvent être copiés sur un support amovible vierge. Ceux-ci pourront éventuellement être traités plus tard

à des fins de récupération en gardant à l'esprit que leur intégrité et leur innocuité ne peuvent être assurées.

Bloquer les nouvelles infections sur la base des éléments connus

Lorsque le programme malveillant qui a réalisé l'infection est identifié, il est possible de rechercher sur Internet ou dans les journaux du système d'information des éventuelles caractéristiques de celui-ci (URL utilisées, nom de fichier, sujet du courrier électronique, etc.). Ces éléments peuvent être utilisés pour éviter d'autres infections. Des actions peuvent notamment être entreprises sur les passerelles de messagerie, les passerelles de navigation sur Internet ou les serveurs de boîte aux lettres.

Restaurer le système depuis des sources saines

La machine ayant été infectée par un programme malveillant, l'intégrité du système peut d'autant plus être mise en doute. Plutôt que d'espérer qu'un éventuel utilitaire de désinfection ramène le système dans un état sain, il est préférable de réinstaller le système depuis un support connu et de restaurer les données depuis les sauvegardes ayant préalablement été effectuées. L'efficacité ou l'innocuité de méthodes de nettoyage alternatives sont difficiles à qualifier. Le vecteur initial de propagation doit par ailleurs être corrigé après réinstallation des systèmes, afin d'éviter une nouvelle infection : application des correctifs de sécurité, changement des mots de passe, modification du pare-feu local, etc.

En l'absence de sauvegarde, rechercher la disponibilité de méthodes de recouvrement des données

Comme cela a été mentionné, des défauts de conception des rançongiciels sont parfois découverts et peuvent permettre un recouvrement total ou partiel des données. Si les données victimes n'ont pas été préalablement sauvegardées et que leur niveau d'importance le justifie, un dernier recours peut être de rechercher d'éventuels utilitaires de recouvrement, proposés notamment par les éditeurs d'antivirus. Cependant, il faut faire preuve de vigilance et qualifier la provenance de ces utilitaires, car ceux-ci pourraient se révéler malveillants et provoquer une surinfection.

Ne pas payer la rançon

Outre le fait que payer la rançon entretient le système frauduleux, le paiement ne garantit nullement l'obtention d'une quelconque clé de déchiffrement ni la sécurité des moyens de paiement utilisés.

DOCUMENT 6

Le shadow IT (Technologie informatique fantôme).

Les collectivités territoriales face à la cybercriminalité - Fiche n° 8 - ANDCDG Edition 2016.

- **Synthèse**
  - Côté gestionnaire du système d'information : cerner les besoins des utilisateurs pour mettre des solutions validées, en adéquation avec leur besoin, à leur disposition
  - Côté utilisateur : remonter les besoins pour l'accomplissement des missions avec le plus de clarté possible pour être compris par les acteurs du système d'information
  - Ne pas restreindre de manière trop drastique tous les usages des ressources IT au sein du SI pour ne pas générer « d'envies de contournement »

Derrière cette dénomination barbare se cache un phénomène complexe à gérer au quotidien pour un administrateur, à savoir des éléments déployés par les utilisateurs sans en référer à la DSI.

Cela va de l'utilisation des BYOD (voir fiche n° 6) à des choses plus problématiques dans le contrôle des données générées par la structure, comme la mise en place d'un « cloud » non répertorié, le déploiement de matériel non référencé, l'intervention d'informaticiens extérieurs à la structure et le plus important en termes de chiffres les macros Excel non validées. Cette liste est non exhaustive et tous les jours, les méthodes de communication permettent de nouvelles possibilités de développer ce phénomène.

A ce titre, une partie de l'information échappe complètement au gestionnaire du système d'information, les sauvegardes ne sont plus assurées et la potentialité de perdre des données augmente avec le nombre d'utilisateurs du service « hors cadre ».

Les logiciels non répertoriés sont aussi une composante importante du shadow IT, ils répondent à un besoin immédiat de certains utilisateurs et représentent un risque dans le sens où la solution n'a pas été testée ni approuvée en termes de sécurité et génère des données non contrôlées.

Le retour arrière sur des applications de ce type est quasiment impossible, les données n'étant pas répertoriées officiellement, elles ne sont donc pas intégrées dans le cycle de sauvegarde du système d'information. Malgré tout, cet état de fait est révélateur d'un besoin des utilisateurs qui n'est pas forcément toujours pris en compte par la DSI.

Le temps des utilisateurs passifs des SI est révolu, la culture numérique prenant de plus en plus d'ampleur. Les méthodes de substitution pour un outil manquant sont de plus en plus accessibles à ces derniers qui n'hésitent plus à sauter lepas de l'installation.

Malgré tout, les dangers liés à cette pratique sont bien présents. Dans le cadre de l'exploitation d'un logiciel tiers non validé, la perte de données est une menace constante. Ces logiciels sont souvent installés sur un poste de travail qui n'a pas de moyen de sauvegarde et ne présente aucune sécurité accrue de fonctionnement, contrairement aux serveurs. La panne technique peut donc être fatale aux données générées par l'application.

Dans le cadre d'adjonction de matériel non répertorié, le risque est tout aussi grand. Il passe de la mauvaise installation/utilisation du matériel à un usage inapproprié qui pourrait mettre en danger le SI. Dans le cadre des macros Excel, elles peuvent aller à l'encontre de la politique de sécurité qui consiste par défaut à les désactiver pour éviter des attaques par ce biais. Elles peuvent aussi être plus pernicieuses en générant elles-mêmes une faille sur une mauvaise implémentation.

Dans le cadre des BYOD, un smartphone peut très bien être utilisé en modem pour contourner des règles jugées trop restrictives. Dans ce cas précis, l'exposition est maximale par rapport

à la sécurité car l'adjonction de ce point d'entrée Internet non géré et surtout non contrôlé augmente terriblement la surface d'attaque.

Les exemples ne manquent pas entre les BYOD et toutes les nouvelles technologies de communication et de partage. La solution reste de travailler en étroite collaboration les uns avec les autres. L'expression des besoins doit être faite en temps et en heure de la part des utilisateurs, et le gestionnaire du SI doit s'efforcer d'y répondre de son côté dans la mesure du possible.

Cela reste la meilleure des manières de ne pas avoir besoin de recourir à des éléments externes au SI. Malgré tout, le gestionnaire doit rester vigilant et en écoute pour essayer de détecter tout élément étranger à son réseau pour pouvoir, le cas échéant, prendre des mesures face au déploiement de tels dispositifs.

DOCUMENT 7

5 conseils à suivre pour être en conformité avec le RGPD.

Journal du net - Lacy Gruen - Novembre 2017.

À partir de mai 2018, toutes les entreprises traitant des données à caractère personnel devront être conformes au nouveau règlement. Quelques conseils pour se mettre à jour.

Le RGPD (Règlement Général sur la Protection des Données) est un texte européen qui traite de la protection des données à caractère personnel des personnes physiques résidant en Union Européenne. Quel que soit le pays où se trouve le siège social d'une entreprise, celle-ci doit être conforme au règlement si elle récolte les données de citoyens européens. L'Europe expose clairement ses attentes en matière de sécurité, mais n'explique pas clairement la marche que les entreprises doivent suivre pour s'y conformer.

Les techniques et technologies utilisées par les entreprises pour sécuriser leurs données sont différentes selon leur activité. Néanmoins, elles doivent élaborer des méthodes pour pallier leur vulnérabilité en matière de sécurité et pour mettre en place de nouvelles façons de les collecter, de les traiter et d'y accéder.

1. Limiter les risques de l'exposition des travailleurs mobiles

Le nombre de travailleurs nomades est en constante augmentation. En effet, via de multiples périphériques, ces travailleurs accèdent régulièrement à des applications et services basés dans le Cloud, depuis n'importe où dans le monde.

Pour limiter les risques sécuritaires que cette mobilité implique et contribuer à assurer la conformité au RGPD, les entreprises doivent mettre en place de nouveaux contrôles et de nouvelles politiques en tenant compte du contexte. Le contexte comprend l'espace de travail de l'utilisateur et les risques de sécurité qu'il pose en fonction de son emplacement, du périphérique connu ou inconnu, de la fiabilité du réseau et de l'heure de connexion.

Grâce à des contrôles d'accès réguliers, la DSI peut facilement suivre l'accès des utilisateurs et créer des pistes d'audit qui aident l'entreprise à respecter les exigences du RGPD.

2. Réduire et contrôler les accès privilégiés des utilisateurs

De nombreuses organisations accordent des droits d'accès privilégiés à des utilisateurs qui nécessitent une gestion particulière. Ces utilisateurs privilégiés sont les premières cibles des acteurs malveillants car leurs droits d'accès étendus permettent aux pirates de naviguer plus facilement sur les réseaux privés, SI et applications d'entreprise.

Pour réduire les risques, les entreprises doivent être proactives et mettre en place des contrôles d'accès dynamiques. Les droits d'utilisateur privilégiés doivent être immédiatement verrouillés lorsque les administrateurs quittent une application ou indiquent qu'une tâche est terminée.

Par ailleurs, pour une sécurisation optimale des données, la gestion de ces comptes à privilèges permet de déterminer une échelle de criticité des données à caractère personnel. Pour assurer la sécurité de ces comptes, les mots de passe doivent avoir une authentification forte et l'utilisateur doit être obligé de passer par un serveur de rebond pour accéder à ces informations.

3. Diminuer les taux de réussite des logiciels malveillants

Les cybercriminels utilisent les attaques d'hameçonnage par e-mail, sur des sites Web et périphériques mobiles pour transmettre du code malveillant aux dispositifs informatiques et accéder à des données personnelles.

La plupart des organisations ont déjà mis en place une forme de whitelisting, mais l'ajout de contrôles lors des étapes en amont - utilisant des signatures pour ouvrir des fichiers ou exécuter des applications - peut empêcher les utilisateurs de lancer accidentellement une attaque.

Ainsi, le contrôle d'accès à certains sites Web ou fichiers spécifiques empêche les utilisateurs d'enregistrer des fichiers malveillants sur des disques durs locaux et verrouille les périphériques externes, afin que seuls les fichiers protégés ou chiffrés puissent être ouverts ou sauvegardés. Ces contrôles proactifs aident les organisations à assurer la protection des données à caractère personnel et à démontrer qu'elles respectent les exigences du RGPD en matière de sécurité.

4. Constituer des équipes adéquates

De nombreuses organisations font encore appel à des processus manuels pour gérer les parcs machines des travailleurs lors de l'embauche et du licenciement. Ces types de process entraînent souvent des erreurs systèmes.

En effet, des études ont montré que de nombreux travailleurs ont encore accès aux données de l'entreprise après l'avoir quittée - parfois pour une période prolongée –, ce qui met en péril le SI. Il est donc important pour l'intégrité de l'entreprise de mettre en œuvre des processus informatiques appliquant des politiques d'accès automatisées aux applications et SI.

En adoptant une approche plus holistique de la gestion du cycle de vie des identités, la sécurité peut être améliorée considérablement pour aider à répondre aux exigences de conformité du RGPD.

5. Enregistrer tous les accès aux données à caractère personnel pour un suivi précis et des rapports exacts

Les organisations doivent tenir à jour des registres de la collecte, du stockage et du traitement des données à caractère personnel qu'elles récoltent, pour être en conformité avec le règlement.

Une gestion fine et précise des autorisations d'accès est également indispensable. La DSI doit connaître tous les accès dont dispose chaque utilisateur pour protéger les endpoints sur tous les types de terminaux utilisés.

L'implémentation de solutions logicielles qui fournissent des rapports d'audit détaillés sur les espaces de travail est donc primordiale pour le bon fonctionnement de l'entreprise et permettent également d'être en conformité au RGPD.

DOCUMENT 8

Le point sur… le FttO « Fiber to the Office ».

ant.cerema.fr - Aménagement Numérique des Territoires - 15 septembre 2017.

Le point sur ...

Le FttO

«Fiber to the Office»

L'internet et les usages liés aux technologies de l'information et de la communication sont devenus indispensables au marché professionnel. Le volume de données échangées explose : courriels de plus en plus nombreux accompagnés de pièces jointes souvent volumineuses, développement du télétravail et de la visioconférence, externalisation de fonctions comme le stockage de données et les applications en ligne avec le « cloud computing », interconnexion des différents établissements d'une entreprise ou d'une collectivité par des réseaux privés virtuels (VPN) ...

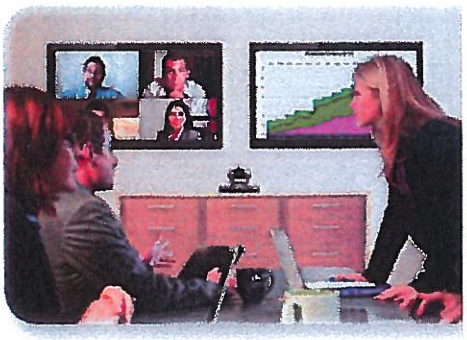
Aujourd'hui, 98 % des entreprises de plus de 10 salariés sont connectées à l'internet, mais la plupart ne bénéficient que de services identiques à ceux qui sont proposés aux particuliers.

Les performances des réseaux de communications électroniques à haut débit via les technologies xDSL deviennent insuffisantes pour permettre l'accès des entreprises aux nouveaux services. Le saut technologique vers la fibre optique qui permet les services fixes à très haut débit doit se faire sans tarder.

Toutefois passer du cuivre à la fibre ne suffit pas : les réseaux FttH (fiber to the home, la fibre jusqu'au domicile) du secteur résidentiel ne sont généralement pas adaptés aux usages et aux exigences des entreprises. Même les offres FttE (Fiber to the entreprise), bâties sur l'architecture FttH, et dont la qualité de service est améliorée, ne pourront répondre aux attentes de certaines, en raison de leur taille ou de leur type d'activité. Leurs besoins sont en effet sensiblement différents de ceux des particuliers : outre des débits descendant et montant symétriques élevés et garantis, elles exigent des conditions particulières nécessaires au fonctionnement de leurs établissements. C'est pourquoi les opérateurs de communications électroniques proposent aux entreprises une offre spécifique, le FttO (fiber to the office, la fibre jusqu'au bureau).

Les besoins en débit des entreprises augmentent

Comme dans le secteur résidentiel, les usages se multiplient et sont de plus en plus gourmands en débit. Les entreprises sont passées de l'envoi de courriels en textes simples, dont le nombre explose par ailleurs, à la réception et à l'émission de courriels au texte enrichi, de fichiers lourds comme des plans, des catalogues ou encore de l'imagerie.



Ainsi, les modes de travail et les pratiques professionnelles évoluent avec

- la numérisation généralisée des supports,
- la visio-conférence de qualité,
- le télétravail,
- l'interconnexion de sites grâce au VPN (virtual private network, réseau privé virtuel) entre filiales, clients et partenaires permettant de travailler en réseau en temps réel depuis différents établissements parfois situés à des milliers de kilomètres les uns des autres,
- l'externalisation d'applications jusque-là concentrées dans l'entreprise (téléphonie d'entreprise, paie, gestion de stocks, CAO...).

Par exemple, en matière d'imagerie médicale, pour transmettre une IRM de 25 Go, il faut plus de 5 heures avec un débit de 10 Mbit/s contre une demi-heure si le débit est de 100 Mbit/s. Avec un débit de 1 Mbit/s, cet envoi devient mission impossible, puisqu'il faudrait 55 heures !

Le cloud computing, ou cloud (le nuage), qu'on traduit par «l'informatique en nuage», consiste à héberger sur des serveurs distants interconnectés des données et traitements informatiques jusque-là respectivement stockés et effectués dans l'entreprise, sur le poste de travail de l'utilisateur ou sur des serveurs locaux. Selon la définition du NIST (National Institute of Standards and Technology), **le cloud computing est l'accès via le réseau, à la demande et en libre-service, à des ressources informatiques virtualisées et mutualisées. Les utilisateurs peuvent ainsi accéder à des services en ligne variés sans avoir à gérer les équipements nécessaires** (les serveurs, la mise à jour des logiciels). Une condition au bon fonctionnement du système : des débits élevés entre clients et serveurs.

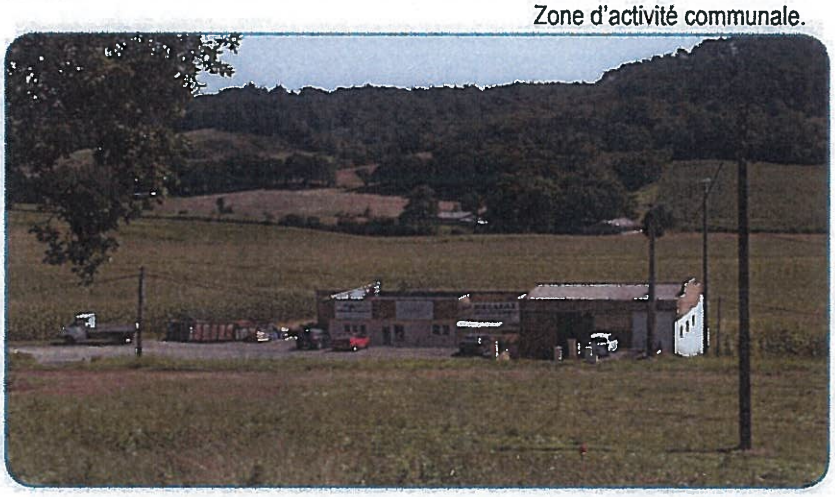
Certains secteurs d'activité nécessitent toujours plus de bande passante, comme les hôpitaux qui ont besoin de débits élevés pour échanger rapidement de l'imagerie médicale, ou les imprimeries, la presse, les agences de communication, les bureaux d'études, les architectes, les ingénieurs qui envoient et reçoivent des fichiers graphiques extrêmement lourds.

Tous ces usages n'existent pas sans connexion au très haut débit.

Or les technologies xDSL atteignent aujourd'hui leurs limites en termes de performances qui sont de quelques Mbit/s en débits symétriques. Seuls les réseaux à très haut débit en fibre optique offrent et offriront dans le futur des possibilités quasi-illimitées répondant aux exigences de qualité de service de l'entreprise.

La fibre apparaît donc comme un levier déterminant et incontournable de développement économique pour stimuler la productivité, favoriser la croissance, initier des usages innovants et créer des emplois.

Zone d'activité communale.



Des usages professionnels qui demandent des services adaptés

Les besoins des entreprises et des établissements publics diffèrent sensiblement de ceux des particuliers, notamment en ce qui concerne

- les débits, qui certes doivent être élevés (100 Mbit/s et au-delà), mais également symétriques (débits montant et descendant identiques) et surtout garantis, sans variation de la bande passante au cours de la journée,
- le temps de réponse (latence), qui doit être le plus réduit possible, de l'ordre de quelques millisecondes,
- la priorisation des flux pour permettre à des applications comme la visio-conférence de bien fonctionner et de ne pas subir de dégradation de l'image quand quelqu'un télécharge un gros fichier,
- la sécurité des échanges,
- la possibilité d'interconnexion de réseaux locaux de sites,
- la garantie de rétablissement rapide en cas de panne (sous 4 heures en général), ce qui implique une organisation chez l'opérateur et une technologie spécifiques,
- l'engagement d'interruption maximale de service (IMS) pour limiter les durées de coupure.

Le FttH (fiber to the home, la fibre jusqu'au domicile), qui s'adresse au grand public, ne répond pas à ces besoins spécifiques, ni même le FttE qui en est dérivé.

La solution existe pour les entreprises et les sites publics : c'est le FttO (fiber to the office, la fibre jusqu'au bureau).

Les déploiements FttO des opérateurs privés

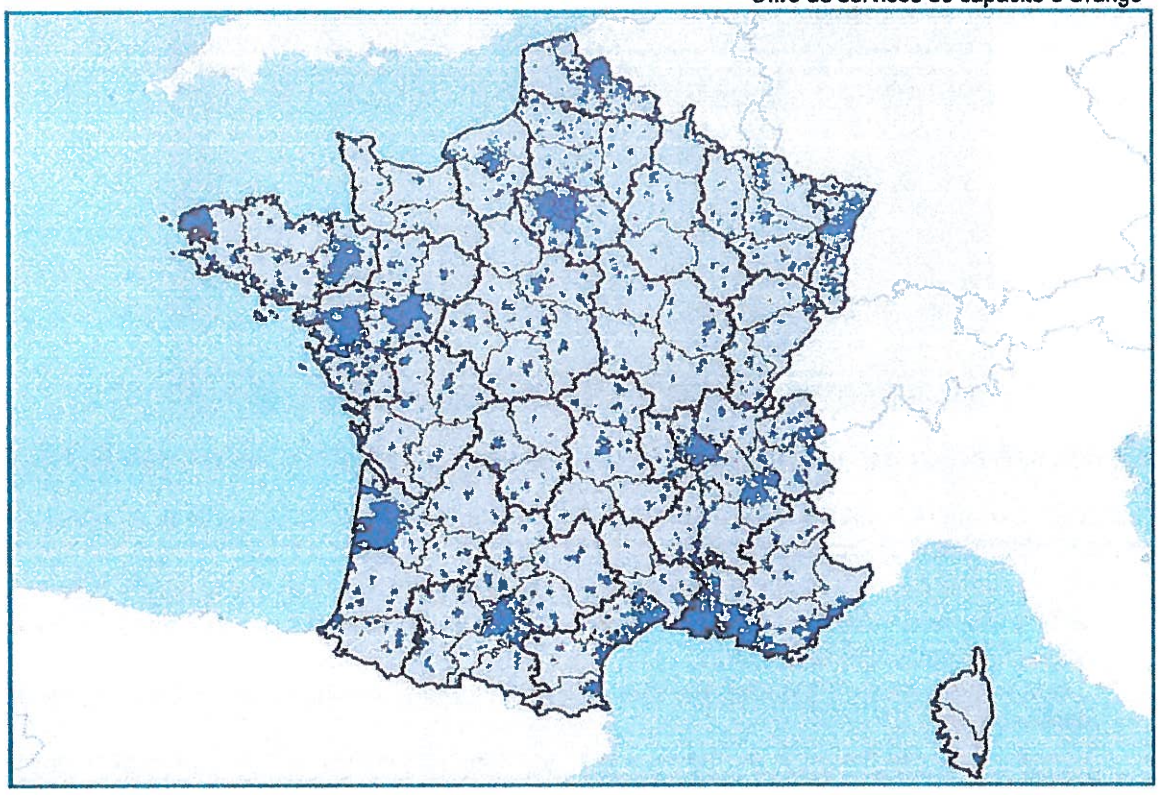
Le nombre d'abonnés FttO se monte actuellement à plus de 60 000 liaisons vers des sites d'entreprises, tous opérateurs confondus.

On peut distinguer sur ce marché deux types de clients professionnels :

- ceux (environ la moitié des entreprises) dont les besoins sont proches de ceux des particuliers soit commerçants, professions libérales, établissements multi-sites raccordés aux réseaux de leurs maisons-mères, se satisfaisant des solutions d'entrée de gamme (ADSL pro, FttH pro et prochainement FttE),
- les entreprises qui ont des exigences plus fortes en matière de niveau et de garantie de service (sièges sociaux, SSII, établissements de soins), ayant aujourd'hui des accès SDSL (« s » pour symétrique) de 4 à 8 Mbit/s progressivement remplacés par des accès FttO offrant un débit garanti et symétrique élevé (10 Mbit/s à 10 Gbit/s).

L'opérateur historique annonce que son réseau en fibre optique dédiée couvre aujourd'hui 6 500 communes dans lesquelles il est en mesure de proposer le raccordement du site client à tarif forfaitaire, les communes étant classées dans trois zones tarifaires aux tarifs croissants O1, O2 et O3.

Offre de services de capacité d'Orange



Les tarifs d'abonnement restent quant à eux dépendants des besoins propres de chaque entreprise cliente. En outre, les services basés sur l'architecture FttO font l'objet d'une offre de gros régulée d'Orange. Tous les opérateurs dédiés au marché entreprises y ont accès afin qu'ils puissent bâtir des solutions techniques qui répondent aux besoins de leurs prospects ou clients.

SFR raccorde, avec sa propre fibre, le ou les sites des entreprises dans une quarantaine d'agglomérations grâce à son propre réseau ainsi qu'à ceux déployés par Completel avant son rachat par Numericable.

Début 2011, **Orange et SFR** se sont engagés à déployer leurs réseaux dans 3 500 communes moyennement denses. Dans ces communes, les zones d'activité économique desservies par SFR font l'objet d'un traitement spécifique : les points de mutualisation ainsi que le réseau horizontal sont dimensionnés de manière à permettre le déploiement d'une fibre par entreprise (FttO). Le raccordement est réalisé lors de la demande de l'opérateur de service, après étude, la tarification étant fonction des infrastructures mobilisables. **Bouygues Télécom** a commencé à commercialiser des offres FttO destinées aux entreprises au printemps 2013. **Colt Télécommunications** présente en région parisienne, à Lyon, Toulouse ou Marseille, propose des services aux entreprises de toutes tailles.

FttO et réseaux d'initiative publique

Force est de constater un certain manque d'appétence des entreprises pour le FttO, en raison principalement du coût élevé des frais de raccordement, et de celui des abonnements. C'est particulièrement le cas des **petites entreprises qui jugent ces coûts sans rapport avec leurs besoins et se trouvent ainsi exclues du bénéfice du très haut débit**.

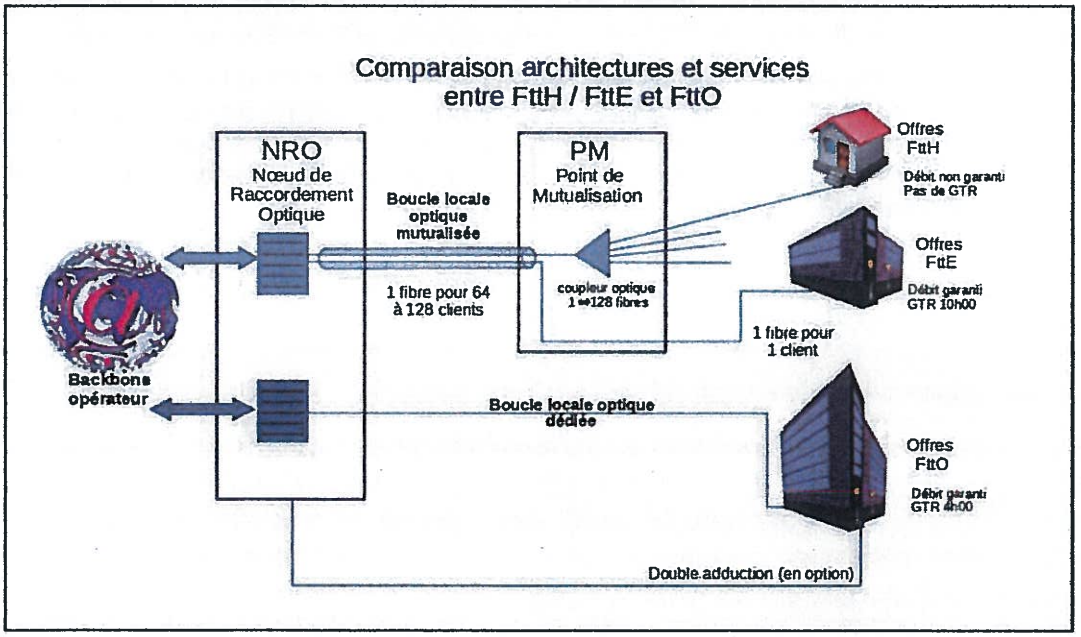
Cette situation a conduit les collectivités à déployer des réseaux d'initiative publique (RIP) pour assurer la desserte en FttO de leurs entreprises en apportant une concurrence sur les tarifs et les services, cela depuis que la Loi pour la confiance dans l'économie numérique, de 2004, les a autorisées à établir et exploiter des réseaux de communications électroniques. Il se trouve qu'aujourd'hui de tels réseaux sont présents dans certaines zones de déploiement privé (zones AMII).

Les réseaux d'initiative publique locaux proposent systématiquement des offres de gros techniquement plus ouvertes et plus intéressantes au niveau tarifaire que celles des opérateurs privés. Ces réseaux sont ouverts aux opérateurs de service dédiés aux entreprises comme Céleste, Adista, Alsatis....

L'ARCEP estimait dès 2009 que plus de 2 000 zones d'activités étaient fibrées par les RIP.

Quelques exemples :

- en l'absence d'initiative privée pour le fibrage de ses zones d'activité économique, la Communauté d'Agglomération de Sarreguemines Confluences a choisi de construire un réseau optique, exploité en délégation de service public.
- l'agglomération de Poitiers a été amenée à fibrer ses zones d'activité à cause du manque d'intérêt des opérateurs privés pour les sites économiques, tout en laissant le FttH à leur initiative.
- la ville de Vannes a décidé de fibrer jusqu'à chaque parcelle d'entreprise deux zones d'activités qu'elle souhaitait dynamiser.
- dans le département de l'Oise, le réseau Téloise dessert 75 ZAE.



Et demain ?

Les opérateurs SFR et Orange ont signé fin 2011 un accord pour se répartir la couverture des 3 500 communes dans lesquelles ils se sont tous deux déclarés prêts à déployer un réseau FttH d'ici à 2020. A l'occasion de ces travaux qui concernent majoritairement le secteur résidentiel, **les opérateurs doivent prévoir des architectures de réseaux permettant d'assurer également la desserte FttO des entreprises situées dans le tissu urbain.**

Les opérateurs qui couvrent une zone arrière de point de mutualisation doivent déployer leur réseau sur la totalité de cette zone pour respecter obligation de complétude inscrite dans la réglementation FttH. Ces déploiements amènent alors des réseaux FttH dans des secteurs où des offres FttO sont d'ores et déjà disponibles. Le risque existe donc de voir certains abonnés FttO considérer que ce que leur coûte leur liaison en fibre optique dépasse leurs réels besoins (garanties de débit et de rétablissement rapide notamment), et donc se reporter sur une offre FttE. Une telle offre leur apporterait à moindre coût une bande passante suffisante pour répondre à leurs besoins.

Fibrage d'une rue commerçante à Nantes

La régulation du marché des offres de communications électroniques pour les entreprises

En 2017, l'Autorité de régulation des communications électroniques et des postes (ARCEP) a révisé ses décisions d'analyse des marchés du haut et du très haut débit pour la période 2017-2020. Elle a constaté qu'Orange continue d'exercer une influence significative sur le marché du FttO. Par conséquent, ses tarifs continueront d'être régulés sur la majeure partie du territoire. En effet, un niveau de concurrence suffisant n'existe que sur quelques communes (un peu plus d'une vingtaine jusqu'ici) que le régulateur identifie à partir de critères qu'il a établis dans lesquelles les tarifs sont libres (la ZF1).

En dehors, en ZF2, l'ARCEP exerce un contrôle ex ante sur l'offre de gros à laquelle tous les opérateurs alternatifs ont accès. Dans sa décision de 2017, le régulateur interdit à Orange de « pratiquer des tarifs susceptibles d'évincer sur cette zone un opérateur concurrent efficace construisant sa propre infrastructure » et lui impose également « une obligation de non-excessivité des tarifs pratiqués sur le marché de gros dans la ZF2 » afin de permettre le développement d'une concurrence par les infrastructures.

A voir aussi ...

Sur le site internet Aménagement Numérique des Territoires

- fiche le point sur ... projets de RIP THD : troisième bilan
- fiche le point sur ... FttH point-multipoint passif (PON)
- fiche le point sur ... FttX : le réseau optique de desserte

Sur le site de l'Arcep, l'Observatoire Arcep THD.