INFRALLIANCE

VADEMECUM

DE SOUVERAINETÉ NUMÉRIQUE PAR LES INFRASTRUCTURES

1. Manifeste

La mission de notre Think & Do Tank est de contribuer, par l'angle de l'infrastructure et au travers d'actions concrètes, à l'émergence et à la pérennité d'une troisième voie, vers les souverainetés numériques inclusives, pour une autonomie de destins des pays européens.

Considérant que la souveraineté numérique se définit et se construit par l'action, répondant itérativement au besoin d'acculturation et de solutions des usagers et des institutions, la vocation d'Infralliance est d'accompagner, à l'échelle des couches infrastructurelles, les organisations publiques et privées dans la compréhension des enjeux relatifs aux données numériques et d'imaginer, de proposer et de mettre en pratique des évolutions d'usages et des solutions adaptées en termes de risques et de data continuum.

Attachés au principe de réalité et aux interprétations factuelles, nous optons pour la progression par petits pas et pour l'esprit de partenariat, y compris avec certains acteurs non européens et ce, au-delà même de notre co-fondateur japonais, Telehouse, incarnant l'accord bilatéral de libre-échange euro-japonais sur le volet de la souveraineté numérique.

Car ce n'est pas la construction d'un carcan numérique européen qui nous anime, mais plutôt le développement et le partage de pratiques calibrées et de solutions adaptées et concrètes, permettant à chaque entreprise, territoire ou Etat, d'accéder à un niveau de souveraineté qui soit à la hauteur de ses enjeux sécuritaires et sociaux économiques spécifiques.

Notre vision est celle d'une souveraineté numérique ancrée dans le réalisme et l'ouverture. Les acteurs des continents actuellement dominants (Asie dont la Chine, Amérique du Nord) sont des sources d'inspiration et de synergies potentielles et non d'opposition systématique. Pour autant, la bienveillance n'est pas naïveté et la réalité des rapports de force doit être intégrée aux réflexions, choix et arbitrages qui guident nos projets, prises de positions et actions.

Avec les autres groupes de travail, think et/ou do tanks, avec les acteurs des couches hautes et surtout avec les usagers, nous œuvrons par l'écoute, l'intelligence collective et l'association de compétences, servant ainsi notre sens pratique pour la co-construction, brique par brique, de la mosaïque des usages qui définiront la sécurité et la pérennité des souverainetés numériques de demain.

Gabriel Chenevoy
Directeur général de Terralpha

Franck Simon
Président de France-IX

Sami Slim
Directeur général de Telehouse France

2. Prise de position des cofondateurs d'Infralliance sur la souveraineté numérique

Franck Simon,
Président
de France-IX

Préalablement à toute approche relative à la souveraineté numérique, il convient de rappeler que l'Ingénierie d'infrastructures consiste en un assemblage maitrisé des offres et des techniques proposées par les nombreux acteurs et partenaires de la chaine de valeur. Ce point fondamental sous-tend que la souveraineté des données passe par la maitrise des niveaux d'Infrastructure. *(Au-delà du risque, le lien entre souveraineté et résilience est très important.)*

Trois points sont ainsi capitaux :

- La maitrise des partenaires opérateurs : Datacenter, opérateurs fibre, fournisseurs d'équipements et de leurs sous-traitants (RGPD, partage des données…) qui doivent tous être « validés », sans quoi il n'y a pas de souveraineté possible.
- La redondance des infrastructures à l'intérieur du datacenter : les fibres, les baies, les châssis ou encore les alimentations électriques. Lorsqu'un client est connecté sur plusieurs ports, il est essentiel de répartir d'office ses données sur plusieurs cartes dans des châssis différents et éviter ainsi la présence de SPOF (Single Point Of Failure).
- Le choix des partenaires techniques et des équipementiers de confiance dont les garanties sont fortes et qui sont capables de certifier que les données, qu'elles soient sensibles ou personnelles, ne puissent être ni interceptées ou maltraitées. Notons à ce titre que tout changement intempestif de sous-traitant (non vérifiable) est susceptible d'entrainer une résiliation pure et simple du contrat sans préavis et indemnité de la part du client.

La complexité de la souveraineté numérique ne s'arrête toutefois pas à ces dispositions. Des considérations plus ou moins spécifiques, selon le métier et la position que l'on occupe dans cette industrie, peuvent être prises en compte.

A titre d'exemple, France-IX a choisi Nokia pour le renouvellement de son cœur de réseau, notamment pour répondre aux demandes de ses clients américains qui exigeaient des solutions (non chinoises) susceptibles de garantir la qualité de support et un transit sûr et résilient des flux.

Le chemin / continuum de la donnée doit être parfaitement connu pour faire face à d'éventuelles erreurs humaines, défaillances techniques ou actes de malveillance.

C'est pour cela que nous demandons systématiquement aux opérateurs avec lesquels nous collaborons, les fichiers KMZ des parcs de nos clients. Nous pouvons ainsi vérifier si les fibres sont enterrées, protégées ou si elles passent à proximité d'endroits potentiellement sensibles. Tout est contrôlé de manière à évaluer la fiabilité de l'installation (tests optiques).

Puisque les flux de nos clients qui passent par notre plateforme d'interconnexion sont variés, évolutifs et la plupart du temps non prédictibles, nous garantissons un niveau de fiabilité très élevé et fournissons les plus hauts niveaux de SLA (Services Level Agreement), cohérents avec la nature et la sensibilité des services qui passent « dans les tuyaux ». Nous assurons le circuit entre le vendeur et l'acheteur.

Nous prenons en considération le niveau de services du vendeur jusqu'à l'acheteur : quelle bande passante ? quel niveau de disponibilité ? Certaines demandes (au taux de fiabilité désiré de 100%) peuvent déboucher sur la configuration de deux circuits infrastructurels différents de bout en bout, afin de garantir la disponibilité et la résistance à tous types de problèmes.

La protection des données étant au premier rang de notre vision de la souveraineté, nous nous sommes également mis en conformité avec le RGPD des données de nos clients, nécessaires à la réalisation de nos prestations.

Nous avons fait évoluer nos process internes (enregistrés dans notre cahier des registres), no(s) système(s) d'information dont notre messagerie mais également notre site Internet. Nous avons également invité nos prestataires à montrer patte blanche sur l'ensemble de ces aspects.

Le réalisme est tout aussi essentiel que tout ce qui précède : la fiabilité absolue d'une infrastructure coûte une fortune et ne peut garantir à aucun moment un retour sur investissement. Il faut trouver un compromis raisonnable entre résilience et optimisation. Eviter d'avoir des infrastructures qui seraient tellement résilientes qu'elles en deviendraient inutiles, superflues et déraisonnables tant sur le plan financier qu'écologique.

Chez France-IX, nous avons banni les architectures « Full Mesh » pour privilégier au niveau national et régional, des infrastructures en double étoile, les plus optimales pour avoir cet effet [résilience X redondance], sans consommer trop d'électricité et de ressources.

Enfin, de manière plus générale, il faut avoir en tête que :

- Il n'y a de résilience que si elle est traitée de bout en bout de la chaîne.
- Les couches physiques les plus basses doivent être fiabilisées, avant même d'ajouter des couches applicatives supplémentaires de services.
- Les accès aux données, notamment celles qui sont hébergées dans le cloud, doit également être sécurisés. La certification des Data Center (TIER 1 à 4) et leur fiabilité sont une des principales clés de cet enjeu.
- La lecture exhaustive et soignée des contrats, y compris des annexes (que souvent personne ne lit), est vivement recommandée lors du choix d'infrastructure. Lorsqu'on cherche sécurité et résilience il faut porter le regard au-delà du prix proposé.

Avec Infralliance, nous prônons en ce sens la transparence des informations, une obligation de publication de la part des opérateurs. Je souhaite une accessibilité facilitée pour les clients.

Gabriel Chenevoy,
Directeur général
de Terralpha

Terralpha
SNCF RÉSEAU

La souveraineté numérique est un enjeu crucial pour garantir notre autonomie dans nos choix. Avec l'avènement du numérique, notre indépendance spirituelle, intellectuelle et matérielle dépend de plus en plus de notre aptitude à maîtriser les données, les applications et les infrastructures numériques. Par exemple, le réseau social TikTok a une capacité d'influence considérable sur les valeurs et les comportements, qui peut dépasser celle véhiculée par les livres ou les discours. C'est pourquoi les données et les applications sont très surveillées, que ce soit en termes de propriété intellectuelle ou d'implication des Etats dans les opérations de rachats. Les infrastructures le sont, quant à elles, un peu moins.

On ne peut que « tendre » vers la souveraineté numérique. En ce sens il est important de distinguer les éléments critiques pour notre autonomie de ceux qui ne le sont pas. Certains éléments ou composants dans le continuum de la donnée ne sont pas forcément stratégiques. A titre d'exemple, le choix d'une prise fabriquée en Chine n'est pas un élément décisif en la matière et n'impliquera pas interception, modification ou destruction des données.

La souveraineté doit être envisagée à l'échelle européenne plutôt que nationale, car les enjeux numériques ne connaissent pas de frontières.

Plusieurs leviers permettront de renforcer notre autonomie numérique : la prise de conscience de l'importance du sujet, la mise en place de politiques publiques adaptées, la localisation des compétences, la chaîne d'approvisionnement sans oublier la qualité des acteurs dont la survie et le mode de financement peuvent se jouer sur une ligne européenne tout en ayant une présence à l'international.

Dans le même temps, il faut reconnaître les obstacles à l'accès à cette souveraineté. Faire coexister différents continuums de données sur des sujets à forts enjeux est complexe. Peu d'organisations ont des mécanismes permettant d'identifier les différentes typologies de données en fonction du niveau de risque et peuvent ensuite les orienter sur des continuums spécifiques.

Une organisation avertie a plusieurs hébergements pour garantir la sécurité de ses données mais rares sont celles (à l'exception des grandes entreprises) qui ont des messageries différentes (classification C4 et C1) en fonction de l'importance des données échangées. Pour exemple, la métadonnée d'une photo peut être une donnée névralgique si cette dernière renseigne la localisation d'un équipement stratégique.

Il faut donc pouvoir classifier une donnée pour la protéger en fonction de sa sensibilité en y intégrant les limites d'usages liées à sa classification. Le travail du CSF (Comité Stratégique de la Filière Industries de sécurité) est en ce sens décisif.

Les solutions proposées doivent être facilement paramétrables pour ne pas alourdir le quotidien de l'utilisateur et caractérisées par une triple facilité : détection, décision et mise en œuvre.

Dans tous les cas, il est illusoire de viser une architecture numérique 100% européenne. Il y aura toujours des arbitrages à faire notamment entre la robustesse de l'infrastructure et la sensibilité des données. Il est essentiel d'identifier les niveaux où nous avons besoin de plus d'alternatives, de solutions et de fonctionnalités dans le continuum de la donnée.

C'est là l'un des objectifs d'Infralliance : identifier des espaces où des idées et des voies d'innovation pourraient émerger, en se mettant à la place d'un capital risqueur en attente de ruptures pertinentes.

Aujourd'hui, la confiance dans les actions de chiffrements est quelque peu immodérée, notamment dans le secteur du cloud, mais le continuum n'est pas 100% européen, loin de là.

Avec l'informatique quantique, la fracture du chiffrement va permettre dans ce domaine des choses insoupçonnables. Lorsque le mur sera franchi, tout ce qu'on croyait à l'abri ne le sera plus. Une approche multifactorielle est plus que jamais nécessaire. A n'en pas douter elle passera par la souveraineté des infrastructures.

Sami Slim,
Directeur général
de Telehouse France

TELEHOUSE

De nos jours, les acteurs de l'IT sont invités à piloter leur activité en tenant compte des risques. Le pilotage par le risque a créé une tendance significative sur le marché actuel, mettant en avant l'importance de la cybersécurité.

Chaque CTO est maintenant chargé de piloter les risques liés à la sécurité et à l'IT, ainsi que de veiller à la continuité de l'activité. Cette situation amène à une réflexion : quels sont les risques en termes de souveraineté applicables à l'IT ? Comment puis-je les répertorier de manière exhaustive ? Quels choix d'infrastructures dois-je faire ? Comment puis-je procéder, sachant que le risque et la résilience engendrent des coûts IT importants ?

Aujourd'hui, qualifier l'indépendance d'une structure IT par rapport à des entités étrangères est extrêmement complexe. L'IT est fragmentée en plusieurs couches d'abstraction, notamment dans le cloud, qui sont extrêmement attrayantes (pas de dépenses d'investissement) et utiles au quotidien (solutions fluides, flexibles, start & stop, tout-en-un).

En réalité, le CTO s'expose à une perte de contrôle, en particulier en ce qui concerne la souveraineté et à l'extraterritorialité de certaines juridictions.Il est important de rappeler que la souveraineté commence par l'infrastructure, la couche la plus fondamentale, c'est-à-dire les fibres, les centres de données et les premiers équipements qui constituent les bases de l'internet.

Ce sont ces bases qui pourraient être menacées en termes d'intégrité ou même prises sous le contrôle d'une entité étrangère à l'organisation.

En prenant du recul, il est aisé de se rendre compte que les grands blocs mondiaux, tels que les États-Unis et la Chine, qui dominent la technologie aujourd'hui, ainsi que les blocs de second rang, tels que l'Union européenne, le Japon, l'Inde et plus largement les BRICS, s'organisent pour mettre en place une approche à la fois juridique, sécuritaire et technologique de contrôle de l'IT, notamment en se concentrant sur les infrastructures.

Chaque CTO en France et en Europe doit prendre conscience qu'aujourd'hui, des blocs économiques étrangers contrôlent potentiellement les flux d'informations et la technologie que les CTO sont censés maîtriser.

Les blocs américains et chinois adoptent une attitude très offensive et protectionniste. Par exemple, citons le bloc américain qui a initié le Cloud Act, qui étend l'application de la législation américaine à toute infrastructure IT ou technologique, même si elle est opérée en dehors des frontières du pays. À la lumière de cet exemple, le CTO doit aujourd'hui faire face à de nombreuses failles pour piloter son infrastructure en tenant compte des risques.

Piloter le risque pour une personne responsable au sein d'une organisation signifie avoir le choix d'accepter ou de refuser les risques d'extraterritorialité des données, ainsi que la capacité de travailler et de gérer sur le long court en fonction du pays concerné, la résilience de son infrastructure et la façon dont elle fait face à ces risques.

Comment ? En mettant en place des solutions adaptées qui permettent de répondre à ces différents risques, de les atténuer voire de les résoudre lorsque cela est possible. En faisant des choix de sécurité compatibles et cohérents avec la sensibilité des données.

Malgré les rapports de force actuels, il est toujours possible de collaborer avec des organisations américaines ou chinoises sur des aspects moins critiques ou moins sensibles à l'ingérence extraterritoriale. Cela évite la « balkanisation de l'internet », qui est particulièrement limitante sur le plan technologique.

Aujourd'hui, il existe des accords diplomatiques et sécuritaires entre les différents blocs. L'Europe et le Japon ont établi une alliance internationale et signé un pacte de bienveillance qui offre des garanties aux pays et à leurs entreprises en ce qui concerne la non-extraterritorialité des lois, le respect du RGPD, la non-espionnage des câbles sous-marins ou des infrastructures critiques, etc. Ces accords souverains peuvent évoluer avec le temps et nécessitent des mises à jour régulières.

Ces rapports de force et ces accords multilatéraux offrent aux CTO la possibilité de définir un gradient de risque entre les différents pays et de modifier certaines collaborations en évaluant et en notant le risque.

Le CTO n'attribuera pas la même note de risque à un fournisseur japonais qu'à un fournisseur américain ou chinois. Il n'adoptera pas la même approche en matière de résilience avec un fournisseur japonais qu'avec d'autres fournisseurs non européens.

La participation unique d'une entreprise étrangère telle que Telehouse à la cofondation d'Infralliance est un exemple remarquable des relations entre l'Europe et le Japon. Cela montre aux parties prenantes américaines et chinoises un modèle vertueux de collaboration transfrontalière, offrant aux entreprises la possibilité d'être en sécurité et leur permettant de gérer les coûts liés aux risques et à la résilience de manière plus durable.

L'objectif est clair : faciliter les collaborations technologiques transfrontalières (import/export d'équipements ou de licences) tout en réduisant les risques, afin d'éviter des effets collatéraux tels que le « Trump Ban » sur les technologies et les télécommunications chinoises, dont tout le monde se souvient et dont le spectre continue à peser sur l'Europe.

Contrairement aux logiciels, la résilience nationale s'applique plus facilement aux infrastructures telles que les datacenters, qui sont des équipements plus facilement régulables localement. Le cadre juridique s'adapte au cadre du pays d'accueil, en harmonie avec la territorialité des autorisations.

Les datacenters Telehouse assurent la résilience en s'appuyant sur des alternatives canadiennes, japonaises ou brésiliennes en cas de conflit entre blocs.

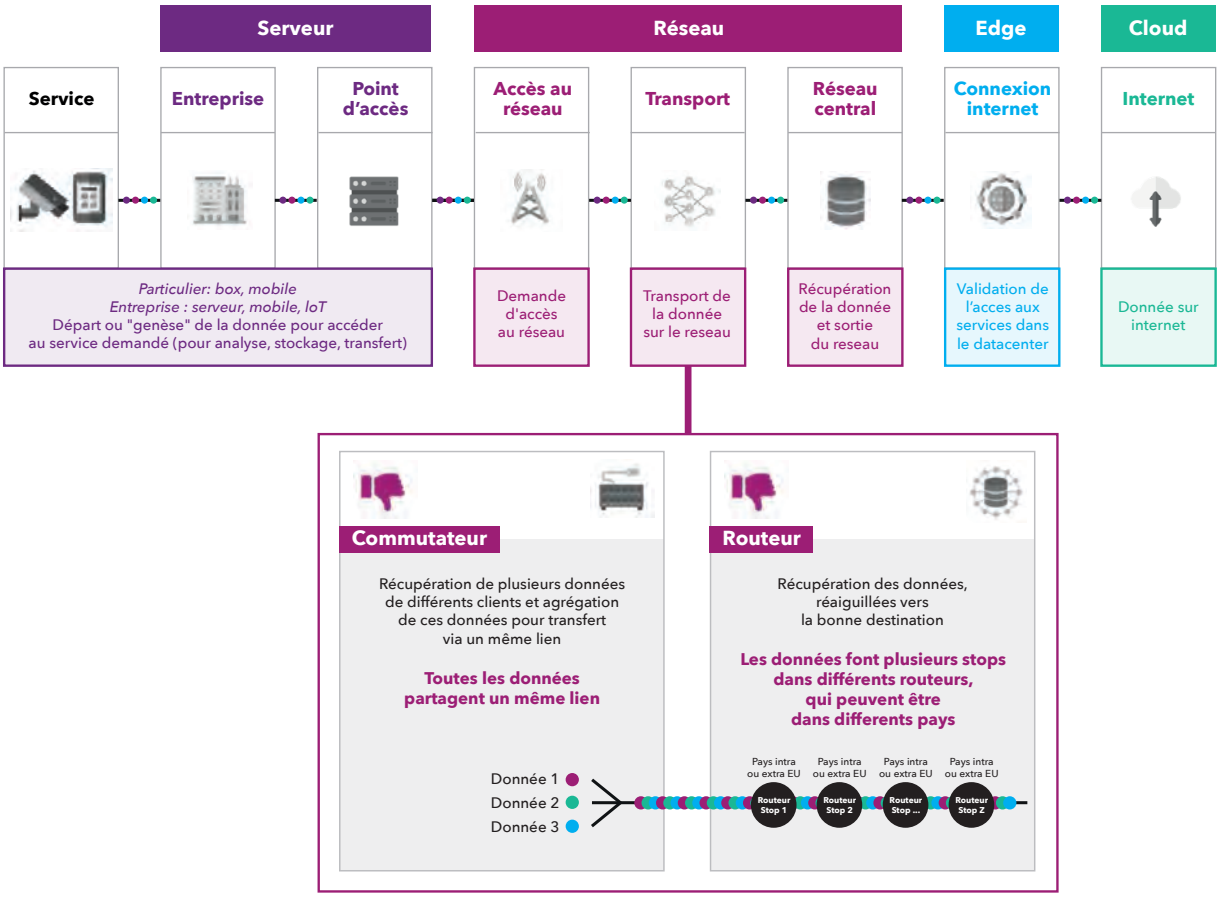
La relocalisation des infrastructures en Europe est également un enjeu important en matière de souveraineté numérique. Relocaliser le trafic Internet permet de redonner du « soft power » aux pays d'accueil en Europe. Lorsque les contenus sont localisés sur nos territoires, cela présente plusieurs avantages. Tout d'abord, sur le plan financier, cela réduit les coûts, car nous n'avons pas à les récupérer. Ensuite, sur le plan juridique, nous avons un meilleur contrôle, car ces contenus se trouvent sur notre territoire national, ce qui nous permet d'agir plus facilement. Enfin, cela favorise la diversité et le choix, car cela encourage la création de contenu local tout en incluant les contenus étrangers dont nous avons besoin.

3. Infrastructures et continuum de la data

Rappel : on appelle infrastructure la composante d'un système qui constitue une **condition préalable** au fonctionnement de ce système.

Parce qu'elles prennent en charge une part essentielle du transport de la donnée, la souveraineté des infrastructures est incontournable dans toute considération souveraine, qu'elle soit politique, technologique, commerciale ou sécuritaire.

Transport de la donnée



4. Typologies de problématiques

L'indépendance numérique se traduit par des décisions concrètes, prises au niveau européen, visant notamment à **développer des solutions** de cloud souverain et des moteurs de recherche locaux mais aussi à encourager les entreprises et autres organisations européennes à prendre leur **indépendance vis-à-vis des grands acteurs transnationaux** du web pour leur préférer des **solutions nationales**.

En regard de l'immense diversité des acteurs, la souveraineté numérique implique également la prise en compte des singularités des différents utilisateur et de leurs enjeux et usages. On peut ainsi différencier les gouvernements, les collectivités territoriales, les organisations dites « sensibles » et bien entendu les entreprises selon leur secteur d'activité. Chaque acteur a des intérêts, des attentes et des contraintes qui lui sont propres et qui préfigurent l'importance et la perspective spécifique de sa problématique de souveraineté.

Une analyse segmentée en cas, par le biais de persona peut alors s'avérer utile pour illustrer le champ des différents enjeux et défis de la souveraineté numérique.

On décrit ainsi des situations concrètes, intégrant différents facteurs, tels que le contexte géopolitique, l'environnement économique, la nature des risques, etc. L'approche proposée ici permet en outre de présenter des mesures ad hoc permettant d'assurer des niveaux adaptés de sécurité et de résilience des systèmes numériques.

Persona 1 Un ministère

Les ministères sont des entités complexes et hiérarchisées qui comprennent souvent de nombreux services et directions. Ils travaillent en étroite collaboration avec d'autres administrations, des organisations publiques et privées, ainsi que des partenaires internationaux pour remplir leur mission.

En tant que représentant de l'État, chaque ministère est soumis à des règles strictes de transparence et de responsabilité. Il doit rendre compte de l'utilisation des fonds publics et respecter les règles et les procédures relatives aux marchés publics et aux appels d'offres. Les ministères ont également pour mission de garantir la continuité du service public, notamment en période de crise.

Problématique

Afin de garantir la confidentialité de ses données et la continuité du service public, le Ministère est à la recherche d'opérateurs télécoms susceptibles d'offrir un service de confiance numérique.

Attentes

- Préservation de la résilience des infrastructures du Ministère en temps de crise
- Respect de SLA exigeants
- Visibilité sur la pérennité et l'actionnariat de l'opérateur
- Interlocuteur(s) dédié(s) aux marchés publics
- Connaissance des règles des marchés publics

Enjeux - contraintes

- Procédure d'appel d'offres : obligation de passer par une procédure pour la majorité des marchés ne permettant pas d'exclure les services non compatibles avec les exigences de confiance numérique
- Processus budgétaires complexes
- Exigence d'un service bout en bout : la boucle locale est généralement imposée par l'opérateur qui répond à l'appel d'offres. Le Ministère n'a pas de contrôle sur la souveraineté et la pérennité des maillons clés de la solution proposée

Solutions et impacts

Un opérateur de transport de données sur longueur d'onde doit pouvoir offrir des solutions en matière de sécurité et de résilience :

- Partie prenante de la sphère publique
- Infrastructure publique et souveraine
- Equipements de transmission d'origine Européenne
- Continuité d'activité en cas de fermeture de frontière
- Supervision 24/7 des équipements actifs et passifs (OTDR actif)
- Chiffrement des données sensibles dès l'infrastructure

Il doit également pouvoir offrir des engagements de moyens spécifiques :

- Equipe dédiée aux projets de marchés publics
- Network opérations Center (NOC) interne et localisé en France
- Flexibilité de facturation

Persona 2 Une collectivité locale

Une collectivité locale est une entité administrative territoriale qui bénéficie d'une certaine autonomie par rapport à l'État central. Les missions et compétences de chaque collectivité locale peuvent varier selon sa taille et son importance, mais elles ont en commun la gestion des affaires locales, en complément de l'action de l'État.

La collectivité locale est donc responsable de la gestion de plusieurs domaines tels que les écoles et les lycées, l'urbanisme, le logement, le transport non urbain, l'environnement, l'aménagement du territoire et le développement économique. Elle s'occupe également de la mise en œuvre des politiques publiques nationales dans le cadre de ses compétences.

En outre, la collectivité locale est une plateforme de participation citoyenne, permettant aux habitants de prendre part aux décisions qui les concernent directement. Elle constitue ainsi un cadre de concertation et de dialogue avec les citoyens pour identifier les besoins et les attentes locaux et adapter les politiques publiques en conséquence.

Problématique

La collectivité locale souhaite réduire la fracture numérique dans le territoire et développer l'économie de sa région pour en augmenter l'attractivité. Elle est à la recherche d'opérateurs télécoms susceptibles d'offrir un service de confiance numérique pour garantir la confidentialité de ses données.

Attentes

- Stockage et traitement local des données
- Visibilité sur la pérennité et l'actionnariat de l'opérateur
- Equipe de proximité

Enjeux - contraintes

- Délais de validation du projet et de construction
- Processus budgétaire complexe qui favorise les investissements (CapEx) vs les abonnements pluriannuels (OpEx)
- Niveau de maturité technique variable en fonction des collectivités locales

Solutions et impacts

Les services d'hébergement pour l'installation de Datacenters de proximité doivent pouvoir offrir des solutions en matière de sécurité et de résilience :

- Partie prenante de la sphère publique
- Infrastructure publique et souveraine
- Services télécoms, énergétiques et fonciers combinés
- Facilite l'engagement de la transition numérique des collectivités
- Favorise l'accès aux réseaux nationaux et internationaux

Ils doivent également pouvoir offrir des engagements de moyens spécifiques :

- Equipe dédiée aux projets d'implantation
- Accompagnement dans la réflexion sur les projets
- Flexibilité de facturation

Persona 3 Un opérateur d'importance vitale (OIV)

Un opérateur d'importance vitale est une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.

Les OIV sont souvent des entreprises ou des organisations qui gèrent ou utilisent des installations critiques pour leur activité, comme des centrales nucléaires, des réseaux de transport d'énergie ou des réseaux de télécommunications.

Le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Les opérateurs d'importance vitale sont désignés pour chaque secteur d'activités d'importance vitale par arrêté du ministre coordonnateur.

Problématique

L'OIV est à la recherche d'opérateurs télécoms susceptibles d'offrir un service de confiance numérique pour garantir la confidentialité de ses données sensibles.

Attentes

- Maitrise du transport de données
- Cœur de réseau sur le territoire français
- Protection contre les lois extraterritoriales
- Visibilité sur la pérennité et l'actionnariat de l'opérateur
- Respect de SLA exigeant
- Stratégie numérique responsable et mesure de l'empreinte écologique

Enjeux - contraintes à dépasser

- Migration des services d'un opérateur vers un autre opérateur
- Niveau de maturité variable sur les problématiques de confiance numérique
- Ressources humaines techniques dédiées manquantes ou absorbées par la mise en place d'approche zero trust network, la migration vers le cloud et le traitement de la dette technique

Solutions et impacts

Un opérateur de transport de données sur longueur d'onde doit pouvoir offrir des solutions en matière de sécurité et de résilience :

- Infrastructure publique et souveraine
- Equipements de transmission d'origine Européenne
- Transport de données sensibles en France
- Couverture nationale
- Continuité d'activité en cas de fermeture de frontière
- Chiffrement des données sensibles dès l'infrastructure
- Supervision 24/7 des équipements actifs et passifs (OTDR actif)

Ils doivent également pouvoir offrir des engagements de moyens spécifiques :

- Engagements RSE mesurables
- NOC interne et localisé en France

Persona 4 Un fournisseur d'infrastructure Cloud souverain

Un fournisseur d'infrastructure Cloud est une entreprise qui propose des services d'hébergement et de gestion de l'infrastructure informatique pour des clients à distance via Internet, en utilisant des serveurs et des équipements de stockage et de réseau déployés sur plusieurs centres de données à travers le monde. Ces fournisseurs permettent aux clients de bénéficier d'une infrastructure informatique à la demande, évolutive, flexible et pay-per-use, ce qui signifie qu'ils peuvent louer et utiliser les ressources informatiques dont ils ont besoin, sans avoir à investir dans l'achat de matériels et de logiciels coûteux, ni à se soucier de la maintenance et de la mise à jour de leur infrastructure. Les fournisseurs d'infrastructure Cloud sont également responsables de la sécurité, de la disponibilité, de la performance et de la conformité de leur infrastructure, ainsi que de la gestion des données et des applications de leurs clients.

Problématique

Réussir à proposer une infrastructure Cloud qualifiée SecNumCloud garantissant une bonne latence réseau et préservant la sécurité et la confidentialité des données de ses clients.

Attentes

Trouver un partenaire d'hébergement et de connectivité réactif susceptible de :

- Respecter les critères stricts définis par l'ANSSI
- Être certifié ISO27001
- Assurer un environnement compatible avec toutes les exigences de la qualification SecNumCloud :
  - un espace technique permettant les configurations adaptées en termes d'alimentation électrique, de climatisation
  - mais aussi un personnel présent 24/7/365.

Solutions et impacts

Mise à disposition d'une salle dans un datacenter :

- respectant tous les critères de la qualification SecNumCloud,
- hautement sécurisée
- étanche à toute intrusion extérieure
- avec un accès contrôlé par un système biométrique
- avec des racks sur mesure selon des contraintes techniques précises.

Persona 5 Une grande entreprise industrielle

Une grande entreprise industrielle est un géant de l'industrie. Elle produit des biens ou des services dans huit secteurs industriels principaux. La construction aéronautique, spatiale et défense, l'automobile, les équipements mécaniques (pièces, machines, outillages, systèmes de production), la construction navale, le ferroviaire, la métallurgie (sidérurgie, fonderie…), les équipements énergétiques puis enfin, l'électrique, électronique, numérique et informatique.

Problématique

Recherche d'opérateurs télécoms susceptibles d'offrir un service de confiance numérique pour garantir la protection de ses données sensibles.

Attentes

- Latence faible
- Capacité dédiée
- Maitrise du transport de données
- Cœur de réseau sur le territoire français
- Protection contre les lois extraterritoriales
- Visibilité sur la pérennité et l'actionnariat de l'opérateur
- Respect de SLA exigeant
- Surveillance et détection des menaces
- Sauvegarde et reprise après sinistre (PRA/PCA)
- Réseau robuste et sécurité
- Chiffrement des données
- Stratégie numérique responsable et mesure de l'empreinte écologique

Enjeux - contraintes à dépasser

- Migration des services d'un opérateur vers un autre opérateur
- Gestion des incidents techniques et de sécurité
- Cybermenaces et attaques
- Complexité de l'infrastructure
- Problématiques de confiance numérique
- Ressources humaines techniques dédiées manquantes

Solutions et impacts

Un opérateur de transport de données sur longueur d'onde doit pouvoir offrir des solutions en matière de sécurité et de résilience :

- Infrastructure publique et souveraine
- Equipements de transmission d'origine Européenne
- Technologies ouvertes à l'innovation des débits et protocoles
- Transport de données sensibles en France
- Couverture nationale
- Continuité d'activité en cas de fermeture de frontière
- Chiffrement des données sensibles dès l'infrastructure
- Supervision 24/7 des équipements actifs et passifs (OTDR actif)
- Options de sécurisation : bascule ou restauration
- Très basse latence et absence de gigue

Ils doivent également pouvoir offrir des engagements de moyens spécifiques :

- Engagements RSE mesurables
- NOC interne et localisé en France

5. Les cofondateurs

France-IX est le premier fournisseur de services d'échange de trafic Internet en France, proposant des services d'interconnexion publics et privés par l'intermédiaire de ses points d'échange neutres (transporteurs et centres de données) à Paris, Marseille, Lille, Lyon, Grenoble et Toulouse ainsi que des services d'hébergement d'équipements, de NAP (Network Access Point), de bande passante (Wave, VLANs) ou encore de formation technique. Le groupe interconnecte plusieurs centaines d'acteurs (opérateurs de télécommunications, FAI, entreprises, fournisseurs de contenu et d'infrastructures de Cloud) et tous les autres réseaux Internet dans le monde entier avec un trafic important sur le marché français de l'Internet. Ses services s'adressent à toutes les organisations qui souhaitent optimiser leurs coûts et leur connexion Internet dans le cadre de leur transformation numérique. Fondée en juin 2010 avec le soutien de la communauté Internet française, France-IX compte aujourd'hui plus de 500 clients et porte les valeurs suivantes : neutralité, durabilité et amélioration constante de l'Internet. Pour plus d'informations, consultez le site web de France-IX : **www.franceix.net**

Telehouse met à disposition de ses clients les datacenters les plus connectés au monde, répartis sur plus de 40 sites dans 19 pays et territoires du globe, couvrant tous les principaux centres financiers et noeuds d'échanges. Telehouse offre une connectivité et une portée mondiales à ses clients, qui ont accès à l'un des écosystèmes d'opérateurs les plus diversifiés en Europe : points d'échange internet, fournisseurs de services cloud, ISP, ASP, entreprises du CAC 40…. Fournisseur mondial de colocation en data center, Telehouse est une filiale du groupe japonais KDDI, entreprise du Global Fortune 500, classé parmi les dix premières entreprises de télécommunications au monde. **www.telehouse.fr**

Terralpha, filiale de SNCF Réseau créée en mai 2021, déploie un réseau alternatif ultra haut débit de haute fiabilité sur le territoire national. Son maillage unique lui confère une résilience, une sécurité et une souveraineté inédites grâce aux fibres optiques posées le long des artères ferroviaires. Pour répondre aux besoins émergeants du Edge Computing et afin de faciliter le développement des centres de données régionaux, Terralpha offre des solutions d'hébergement de DataCenters de proximité dites « Dalles Numériques » qui permettent aux acteurs du numérique un stockage et un traitement local des informations. **www.terralpha.fr**

6. Lexique

CapEx

Le terme «CapEx» est l'abréviation de «Capital Expenditures», qui se traduit en français par «dépenses d'investissement» ou «dépenses en capital». Les CapEx représentent les dépenses qu'une entreprise ou une organisation engagent pour acquérir, améliorer ou entretenir des actifs à long terme, tels que des équipements, des infrastructures, des bâtiments et d'autres éléments nécessaires à ses opérations.

Ces dépenses sont considérées comme des investissements, car elles sont destinées à générer des avantages économiques sur une période prolongée, plutôt que d'être consommées immédiatement. Les CapEx sont distincts des «OpEx» (Operating Expenditures), qui désignent les dépenses d'exploitation courantes telles que les salaires, les fournitures et les coûts opérationnels réguliers.

Les CapEx sont essentiels pour la croissance et le développement d'une entreprise, car ils lui permettent d'acquérir de nouveaux actifs, de moderniser ses installations existantes, d'augmenter sa capacité de production ou d'améliorer son efficacité opérationnelle. Ces dépenses sont généralement planifiées à long terme et nécessitent souvent une analyse approfondie pour évaluer leur rentabilité potentielle.

NOC

Le terme «NOC» est l'acronyme de «Network Operations Center», qui se traduit en français par «Centre des Opérations Réseau». Un NOC est un centre de surveillance et de gestion dédié au suivi et à la supervision des opérations et de la performance des réseaux informatiques, des systèmes, des serveurs, des équipements de télécommunication et d'autres infrastructures liées aux technologies de l'information et de la communication (TIC).

Le rôle principal d'un NOC est de garantir la disponibilité, la fiabilité et la sécurité des infrastructures réseau et systèmes d'une organisation. Les équipes du NOC surveillent en temps réel les indicateurs clés de performance (KPI), les flux de données, les activités de trafic, les niveaux d'utilisation et d'autres métriques pertinentes pour détecter les problèmes potentiels, les pannes ou les violations de sécurité. En cas de problème, les membres du NOC prennent des mesures pour résoudre rapidement les incidents et minimiser les temps d'arrêt.

Les NOCs peuvent être internes à une entreprise, notamment dans les grandes organisations ou les fournisseurs de services, ou ils peuvent être externalisés à des centres de surveillance tiers spécialisés. Ces centres sont souvent équipés d'outils de gestion et de surveillance avancés, ainsi que de personnel formé pour répondre efficacement aux incidents et aux défis techniques liés aux infrastructures informatiques et réseau.

OTDR - Optical Time Domain Reflectometer

L'acronyme «OTDR» signifie «Optical Time Domain Reflectometer», que l'on peut traduire en français par «Réflectomètre Optique à Domaine Temporel». Il s'agit d'un instrument de mesure utilisé dans les réseaux de fibres optiques pour évaluer la qualité et les caractéristiques de transmission de la lumière à travers les fibres.

Un OTDR fonctionne en envoyant un signal lumineux à travers une fibre optique et en surveillant la réflexion du signal causée par les variations d'indice de réfraction et les perturbations sur la fibre. Cette réflexion est appelée «retour d'impulsion», et l'OTDR analyse le temps qu'il faut pour que cette impulsion de lumière revienne après avoir été émise. En utilisant ce temps de retour et la vitesse de propagation de la lumière dans la fibre, l'OTDR peut déterminer la distance jusqu'aux perturbations, aux défauts ou aux ruptures dans la fibre.

L'OTDR est un outil essentiel pour la maintenance, la localisation des défauts et le dépannage des réseaux de fibres optiques. Il peut fournir des informations précieuses sur la longueur de la fibre, les pertes de signal, les connecteurs défectueux, les points de cassure et d'autres anomalies qui pourraient affecter la qualité de la transmission optique. Cela en fait un dispositif important pour les fournisseurs de services de télécommunication, les entreprises qui gèrent des infrastructures de réseau à fibre optique et d'autres professionnels du secteur des télécommunications.

OpEx - Operational Expenditures

Voir CapEx

SLA : Service Level Agreement

L'acronyme «SLA» signifie «Service Level Agreement», que l'on peut traduire en français par «Accord de Niveau de Service». Un SLA est un contrat formel qui établit les attentes, les engagements et les obligations entre un fournisseur de services et son client en ce qui concerne la qualité, les performances et les niveaux de service fournis.

Un SLA définit généralement des objectifs spécifiques en termes de disponibilité, de temps de réponse, de temps de résolution et d'autres paramètres pertinents pour le service offert. Ces objectifs sont souvent mesurés à l'aide d'indicateurs clés de performance (KPI) convenus mutuellement entre les parties. Le SLA énonce également les conséquences en cas de non-respect des engagements, telles que des pénalités financières ou d'autres mesures correctives.

Les SLA sont couramment utilisés dans divers domaines tels que les technologies de l'information, les télécommunications, les services en ligne, les hébergements web, les fournisseurs de cloud computing, et d'autres services où la qualité et la performance sont cruciales pour les clients. Ces accords aident à établir des attentes claires, à favoriser la transparence et à fournir un moyen de mesure objectif de la prestation des services.

INFRALLIANCE

INFRALLIANCE
est le Think & Do Tank
des opérateurs d'infrastructures
pour la co-construction
des souverainetés numériques

contact@infralliance.net

www.infralliance.net

Think et Do Tank infralliance