APIXIT

L'expertise augmentée

Shadow IT : comment garder le contrôle sans limiter les usages ?

Mieux comprendre le Shadow IT pour apporter une réponse sécuritaire adaptée et efficace

LIVRE BLANC Octobre 2018

SOMMAIRE

QUI SOMMES-NOUS ?

APIXIT

APIXIT est l'union des deux spécialistes indépendants des services numériques DCI et RETIS. Expert reconnu des solutions d'infrastructures digitales, de la Digital Workplace, de la Cybersécurité, APIXIT propose un accompagnement global : audit, conseil, intégration en mode projet, services managés.Conscient que l'Innovation est une attente des clients et un atout différenciant, APIXIT est le partenaire privilégié des plus grands constructeurs et éditeurs et porte son attention et son expertise sur les enjeux des organisations et de la transformation digitale.

Animé par une solide culture de la performance, de l'innovation technologique et de la satisfaction client, le groupe APIXIT et ses 350 collaborateurs sont présents à travers toute la France.

CONTACTS

Jean-Philippe GUILLEMIN
Responsable développement d'activité Cybersécurité
jpguillemin@apixit.fr
Tél : 02 99 06 37 02

Céline SALOT
Chargée de Marketing
csalot@apixit.fr
Tél : 02 99 06 31 83

Depuis quelques années les technologies numériques font une entrée fracassante dans les entreprises et les organisations publiques. On les retrouve dans tous les corps de métiers. Plébiscité par de nombreux collaborateurs pour leur simplicité d'usage et souvent disponibles gratuitement dans leur version de base, les services Cloud sont particulièrement représentés. Leur adoption reste cependant trop souvent désordonnée. Les directions informatiques peinent à encadrer les usages et à obtenir de la visibilité sur les applications utilisées par les collaborateurs. Elles sont, au quotidien, confrontées à un dilemme de taille :

Comment favoriser les usages des technologies digitales à des fins d'efficience métiers sans remettre en cause le niveau de sécurité informatique de l'organisation ?

De nouveaux usages numériques s'imposent au sein des organisations

Quand les collaborateurs poussent les organisations à évoluer

En juin 2017, 76% des directions générales interrogées par le groupe Umanis déclaraient que la transformation numérique était un sujet stratégique pour leur organisation. Conscientes de l'enjeu que représente l'intégration des technologies digitales dans leurs activités, nombreuses sont les entreprises qui peinent pourtant à initier des projets concrets et à démocratiser l'usage de ces technologies.

Les salariés, eux, sont très nombreux à utiliser régulièrement des services et des outils digitaux dans leur sphère personnelle. Habitués à de nouveaux usages, ils sont une majorité à les introduire en entreprise. Cette démarche est souvent le fruit d'une initiative personnelle dont la direction informatique n'a pas la connaissance. En effet, 80% des salariés affirment utiliser des solutions informatiques sans l'accord de leur DSI, selon on étude menée par Frost & Sullivan (juillet 2017). Il est d'usage de parler de « Shadow IT » (et plus rarement de « Rogue IT ») pour désigner ce phénomène par lequel des usages informatiques s'effectuent sans l'approbation de la direction informatique.

> Le Shadow IT (traduit en français par l'expression *« informatique fantôme »*) désigne l'usage par les employés de services Cloud non autorisés, généralement dépourvus de contrôles de sécurité robustes, à l'insu du département informatique.
>
> Globbsecurity.fr, février 2018

La pratique du BYOD se généralise également. Les salariés n'hésitent plus à utiliser leurs terminaux personnels (ordinateurs, tablettes, smartphones…) dans un cadre professionnel. Les DSI se trouvent, là encore, confronté à un enjeu de sécurité essentiel puisque le nombre de terminaux utilisé par les collaborateurs croît de façon exponentielle. La gestion des accès au réseau d'entreprise revêt donc une importance toute particulière.

> L'acronyme « BYOD » est l'abréviation de l'expression anglaise *« Bring your own device »* qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel.
>
> CNIL, Février 2015

Une nouvelle génération née à l'ère du digital

La généralisation du Shadow IT et du BYOD est particulièrement soutenue par l'arrivée sur le marché du travail des « digital natives ». Cette génération née avec les nouvelles technologies de l'information et de la communication souhaite pouvoir en bénéficier au quotidien dans le cadre de leurs activités professionnelles. Elle apporte avec elle de nouvelles façons de communiquer et de nouveaux usages que les organisations doivent prendre en compte.

En 2025, la génération Y représentera 75% de la population active.

Source : 3H Coaching

Le Shadow IT, une réponse des métiers à un besoin d'efficience

Le Shadow IT n'est pas un épiphénomène. Il s'agit d'une tendance durable qui devrait même se renforcer dans les années à venir. Une étude menée par NTT Research en septembre 2016 indique que 78% des responsables métiers utilisent des services cloud sans avoir averti au préalable leur direction informatique. Ils sont 83% à vouloir intensifier ces pratiques dans les années à venir. Pourtant cette tendance reste largement sous-estimée par les DSI.

Si l'arrivée de la génération Y dans le monde du travail peut en partie expliquer la tendance du Shadow IT, les raisons qui poussent les directions métiers à adopter des services Cloud en totale autonomie sont plus généralement liées à des problématiques d'efficience métier. 62% des répondants considèrent que le service dont ils ont besoin sera plus rapidement mis en œuvre par leurs soins plutôt que s'ils sollicitent leur direction informatique. Ils sont 52% à penser qu'ils auront accès à une solution plus simple d'utilisation en procédant de la sorte. Enfin, 28% des répondants justifient la pratique du Shadow par une mauvaise compréhension de la part de la DSI de leurs besoins métiers (NTT Research, septembre 2016).

10x

Le Shadow IT est 10 fois plus étendu que ne l'imaginent les départements informatiques.

Source : Skyhigh, février 2018

Stratégie «Cloud First» : quand le modèle *as a service* devient la norme

Convaincues du modèle offert par les fournisseurs de solution cloud (fonctionnalités évoluées, haute disponibilité, administration déléguée, dernières versions disponibles, modèle financier OPEX…), les directions informatiques sont de plus en plus nombreuses à adopter ce type de solutions. Beaucoup d'organisations ont, par exemple, basculé leur service de messagerie dans le Cloud via Office 365 ou Google Apps. L'utilisation de services hébergés tels que Salesforce.com et l'utilisation d'espaces de stockage collaboratifs s'est également démocratisée.

Le cloud computing

23.7%

de services cloud supplémentaires utilisés en moyenne dans les entreprises entre 2015 et 2016

Source : Globbsecurity, février 2018

prend son envol

x3

l'usage actuel du cloud est prêt de 3 fois supérieur à ce qu'il était il y a 4 ans.

Source : Globbsecurity, février 2018

Pourtant, là encore, les utilisateurs semblent avoir pris le pas sur leur service informatique en matière d'adoption du Cloud. Malgré une posture « Cloud first » de plus en plus assumée par les DSI, de nombreuses applications SaaS utilisées dans les organisations reste en dehors de leur contrôle. Le cabinet Frost & Sullivan considère que sur une vingtaine d'applications as a service utilisées en moyenne dans les organisations, sept d'entre-elles n'ont pas reçu l'accord de la DSI (étude menée en juillet 2017).

Quelle influence sur les DSI et le système d'information des entreprises ?

Les rapports entre DSI et directions métiers évoluent

Les tendances décrites précédemment montrent que les métiers agissent de plus en plus souvent en autonomie lorsqu'ils rencontrent des problématiques IT. Une majorité d'entre eux disposent désormais de leur propre budget pour investir dans des technologies digitales.

6/10

DIRECTIONS MÉTIERS

disposent de leur propre budget, totalement indépendant de celui du service informatique pour l'acquisition de solutions collaboratives

Source : IDC France, septembre 2016

La DSI n'est donc plus le décisionnaire unique lorsqu'il s'agit de choisir une solution IT. Une étude menée par CXP Group et Juniper indique cependant, que celle-ci reste la principale responsable de la mise en œuvre des solutions choisies. En effet, 32% des directions informatiques interrogées dans le cadre d'une étude sur l'usage du Cloud Hybride en France, indiquent qu'elles sont le sponsor principal de la stratégie cloud mise en place dans leur organisation (contre 35% pour les directions métiers). En revanche, trois quarts des DSI (76%) sont chargées de la bonne mise en œuvre de la stratégie édictée (étude menée en juin 2016).

Chiffres à l'appui, on observe une évolution des rapports entre les DSI et les directions métiers. Il en résulte une relative perte de contrôle et de visibilité de la DSI sur les technologies utilisées au sein de leur organisation. Cela peut avoir diverses conséquences sur la gouvernance et la sécurité des systèmes d'information.

Un manque de transparence qui rend les systèmes d'information plus vulnérables

La sécurité des solutions as a service reste un des points de blocage principal lorsque l'on évoque les raisons qui freinent les DSI à adopter le cloud. En effet, une grande majorité des services cloud n'est pas en mesure d'assurer un niveau élevé de sécurité et de confidentialité des données. La garantie de niveau de service offert par bon nombre de fournisseurs de solutions cloud ne semble pas à la hauteur des exigences des DSI. Pourtant, comme nous l'avons vu précédemment, les collaborateurs sont très friands de ce type de services. Cela n'est pas sans conséquences pour la sécurité du système d'information de l'entreprise.

Les applications utilisées par les collaborateurs sans que la DSI n'en soit informée peuvent présenter d'importantes vulnérabilités. Méconnues de la direction informatique, celles-ci ne sont pas soumises à la politique de sécurité définie par l'organisation. En outre, aucune procédure de sauvegarde des données n'est, associée à ces applications en cas d'incident technique ou d'incident de sécurité.

8%

DES SERVICES CLOUD

répondent aux exigences de sécurité et de confidentialité des données en entreprise

Source : Globbsecurity.fr, février 2018

En ne se soumettant pas, volontairement ou par facilité, aux règles de compliance édictées, les collaborateurs mettent en péril la sécurité des données de leur organisation. Les applications qui ne présentent pas un niveau de protection validée par la DSI peuvent fournir des portes dérobées qui permettront aux cyber-délinquants d'infiltrer le système d'information. La écurité des données de l'entreprise est alors menacée (compromission ou vol de données par exemple). Les risques sont considérables pour les entreprises, d'autant plus qu'une partie des données concernées par le Shadow IT sont le plus souvent critiques pour le métier de l'entreprise.

80% des collaborateurs estiment que les données qu'ils sauvent sur des services tels que Google Drive, Dropbox ou iCloud sont critiques pour leur entreprise.

Source : NTT Research, septembre 2016

Des initiatives personnelles qui engendrent des coûts cachés

La pratique du Shadow IT n'impacte pas uniquement le niveau de sécurité des entreprises. Cela peut également nuire à leur efficience organisationnelle. En effet, lorsque les utilisateurs comparent, testent et configurent les services qu'ils vont utiliser, ils ne se concentrent pas sur les tâches créatrices de valeur qui leurs sont allouées. Cette démarche est réalisée indépendamment par chaque utilisateur ou service de l'entreprise. Il n'y a, en général, aucune coordination entre les directions métiers. Par manque de transparence sur les usages, les services ne sont pas mutualisés, et aucune optimisation financière ne peut être effectuée.

L'usage de certaines applications peut également perturber l'expérience utilisateur au sein de l'organisation du fait d'une consommation excessive de bande passante ou des effets de bord avec les autres applications (conflits réseaux ou conflits applicatifs par exemple).

Un risque pour votre conformité réglementaire

42%

des utilisateurs reconnaissent prendre le risque de vol ou de perte de données sensibles.

Source : Frost & Sullivan, juillet 2017

41%

des utilisateurs savent que ces données pourraient être exposées à des personnels non habilités.

Source : Frost & Sullivan, juillet 2017

Le nouveau règlement européen sur la protection des données à caractère personnel (RGPD) impose, notamment, de prendre en compte la sécurité des données personnelles dans la conception du système d'information, et l'obligation de signaler les fuites de données suspectées ou constatées. L'usage dissimulé de services dont le niveau de sécurité n'est pas maîtrisé, pourrait mettre à mal la capacité des DSI à respecter cette exigence. La CNIL pourrait alors infliger de lourdes sanctions et notamment une amende pouvant aller jusqu'à 4% du chiffre d'affaire de l'entreprise. L'image de marque et l'attractivité générale de l'entreprise pourrait, en outre, être mise à mal en cas d'incident de sécurité majeur ou de sanction de la CNIL.

LIVRE BLANC

TÉLÉCHARGEZ NOTRE LIVRE BLANC

Pour en savoir plus sur
les prédispositions à prendre pour
être en conformité avec le Règlement
Européen sur la Protection
des Données Personnelles (RGPD)

Comment limiter les risques liés au Shadow IT ?

Le Shadow IT n'est pas un phénomène marginal. Comme nous l'avons présenté, il s'agit d'une tendance lourde présente dans toutes les organisations. Si cette pratique peut avoir des conséquences importantes sur le niveau de sécurité et l'efficience des organisations, il serait utopique de tenter d'éradiquer ce phénomène. Une interdiction des usages IT personnels ne saurait être efficace. Si elles veulent mieux contrôler les usages, les organisations doivent faire évoluer leurs pratiques.

Une direction informatique au service des besoins métiers

Pour mieux encadrer les pratiques informatiques, les DSI doivent être en mesure de comprendre le plus en amont possible les attentes et les besoins des métiers afin de leurs proposer des solutions adaptées à leurs problématiques. Ils doivent se transformer en un véritable fournisseur de services et de capacités pour les métiers. Ils pourront, pour ce faire, proposer aux directions métiers un catalogue riche de solutions innovantes et éprouvées dont ils auront validé le niveau sécurité au préalable. La mise en place des solutions sélectionnées en self-care permettra aux DSI de répondre à un besoin d'agilité très largement exprimée par les métiers. Bien communiquer sur l'existence de ce catalogue de solutions sera primordial pour que les collaborateurs n'aient plus recours à des solutions personnelles.

> Notre premier challenge d'entreprise, c'est d'accélérer ! L'informatique ne peut plus se permettre de freiner le business de l'entreprise. L'idée est de distribuer les accès aux métiers en mode self-service., consommer et déployer à la volée des serveurs, les décommissionner, avoir la même flexibilité qu'on pourrait avoir sur le portail d'une fournisseur cloud.
>
> Rafik KADI, Directeur de projets IT, SODEXO

En procédant de la sorte les DSI peuvent se positionner comme un élément moteur au service de la simplification des usages et des procédures de leur organisation.

Une surveillance accrue des systèmes d'information

Afin de prévenir tout incident de sécurité relatif à un usage non identifié par la DSI, bon nombre de mesures préventives peuvent être prises : installation de firewalls, détection d'intrusion, mise en place d'une politique de sécurité et de gestion des évènements… Le chiffrement des flux d'information (VPN, HTTPS…) associé à un dispositif de stockage des clés de chiffrement fait partie des mesures préventives essentielles à mettre en place. En cas de perte ou de vol de données, celles-ci resteraient inexploitables. Par ailleurs, des audits réguliers du systèmes d'information devront également être réalisés afin de détecter de potentiels incidents ou vulnérabilités.

Le CASB, véritable tour de contrôle de votre système d'information

Comme nous venons de l'évoquer, mettre en place des solutions de sécurisation est essentiel. Cependant, il serait vain de sécuriser le système d'information interne à l'organisation si les collaborateurs stockent leurs fichiers de travail sur des services gratuit hébergés dans le cloud. C'est pourquoi, les fournisseurs de services IT ont mis au point des solutions permettant de sécuriser l'accès aux services Cloud.

85%
des grandes entreprises disposeront d'un CASB dans leur infrastructure en 2020.
Source : Solutionsnumériques.com

5%
d'entre-elles avaient déjà investit dans la technologie en 2016
Source : Solutionsnumériques.com

Il s'agit de passerelles d'accès au Cloud sécurisées nommées CASB (Cloud Access Security Broker) qui s'intègrent entre l'infrastructure sur site des organisations (périmètre du réseau, des périphériques et des données) et l'infrastructure des multiples prestataires services cloud utilisés. Le CASB agit comme une vraie sentinelle qui offre plus de visibilité et de moyens de contrôle aux DSI. Elle leur permet de mieux maitriser les mouvements de données (et notamment de données sensibles) et de sécuriser toutes celles hébergées en dehors du périmètre de l'entreprise sans dévaloriser l'expérience d'usage des collaborateurs. Si peu d'entreprise sont, à ce jour, équipées, nul doute que bon nombre d'entre-elles vont se doter de se type de solutions tant les bénéfices apportés sont importants :

Identification des services cloud utilisés

Le CASB collecte en continue les logs des pare-feu et des proxies et analyse leur contenu. Cela permet aux DSI d'identifier l'ensemble des services cloud utilisés par les collaborateurs. Elles acquièrent de la visibilité sur les applications SaaS « clandestines » et développent une connaissance plus fine des usages grâce à des données granulaires par utilisateur, par activité ou au niveau des données. Cette analyse des comportements leurs permet ensuite de personnaliser des règles par profils.

Evaluation du niveau de risque

Une fois les services cloud recensés, les directions informatiques vont pouvoir s'appuyer sur le scoring établit par le CASB pour évaluer le niveau de sécurité de chacune des applications SaaS. Ce score détermine le niveau de risque en matière de sécurité en se basant sur des dizaines de critères parmi lesquels : le partage de données client avec des tiers sans autorisation, le cryptage des données stockées, les services revendiquant la propriété des données hébergées… Cela accélère considérablement le travail d'évaluation du risque que doivent mener les équipes informatiques.

Mise en oeuvre des règles de sécurité

Une fois cette évaluation réalisée, la DSI peut appliquer des règles de gouvernance des services cloud adaptées. La solution CASB s'intègre avec le pare-feu ou la passerelle Web sécurisée de l'organisation pour faire appliquer ces règles. En général, les applications cloud sont réparties en trois grandes catégories : les services Cloud autorisés, les services cloud tolérés et ceux qui sont interdits. Les directions informatiques peuvent ainsi mieux réguler le Shadow IT et limiter la vulnérabilité de leur système d'information en promouvant les services Cloud utiles à leurs collaborateurs et en interdisant l'accès à ceux présentant un risque sécuritaire important.

Détection des incidents de sécurité

Les règles de gouvernance mises en place au niveau du CASB permettent de bloquer tout transfert de données vers des services cloud non-autorisés. Cela ne signifie pas, cependant, que les données hébergées sur des services autorisés ou tolérés sont protégées contre toute attaque. Il est indispensable de prévenir du mieux possible une exfiltration de données. Les passerelles d'accès au cloud sécurisées offrent un premier niveau de protection. Elles ont la capacité d'identifier des menaces potentielles grâce à une protection basée sur l'apprentissage machine. Les DSI peuvent ainsi s'appuyer sur les solutions CASB pour surveiller leur réseau et détecter dans les meilleurs délai l'apparition de malwares. Grâce aux CASB, il devient plus difficile pour les cyber-attaquants d'utiliser le Cloud comment vecteur d'attaque.

Afin de protéger les données sensibles de l'organisation, il est possible de coupler une solution DLP (Cloud Data Loss Prevention) à la passerelle d'accès au cloud sécurisée. Les données critiques de l'entreprise (données confidentielles ou secretes) sont ainsi ciblées et il devient impossible de les transférer et de les stockées sur des services tels que Google Drive, iCloud, ou encore Dropbox.

Si elle présente de nombreux avantages, la solution CASB ne doit pas pour autant être considérée comme la solution technologique qui répond de façon exhaustive aux enjeux posés par le Shadow IT. Certains risques ne sont que partiellement couverts, il convient de bien garder en tête les limites suivantes :

- La solution CASB analyse les flux qui passent par le réseau d'entreprise et applique la règle qui a été définie en amont par le service informatique. Les flux qui passent par les connexions 4G des smartphones ne sont pas contrôlés par le CASB. Des données d'entreprises peuvent donc fuiter en dehors du réseau d'entreprise par ce biais.

Les services Cloud utilisent régulièrement de nouveaux domaines et de nouvelles adresses IP. Les bases de données des services cloud sur lesquelles les solutions CASB se basent ne sont pas toujours parfaitement à jour et complètes. L'application des règles de gouvernance peut donc être parfois défaillante.

Sensibiliser les collaborateurs aux enjeux de la cybersécurité

73% des salariés déclarent être pleinement conscient d'enfreindre les règles édictées par le RSSI en matière de Shadow IT.

Source : NTT Research, septembre 2016

Il n'existe pas de solution « miracle » pour se prémunir des risques liés au Shadow IT. La technologie ne suffit pas à protéger un système d'information. Une évolution de la culture d'entreprise est également nécessaire. L'interdiction de ces usages devient progressivement anachronique et se heurte à la logique « métier » : seule la pédagogie est de nature à infléchir la tendance. Pour limiter les comportements à risque, il parait essentiel de sensibiliser de façon continue l'ensemble des collaborateurs aux problématiques de cybersécurité et de les responsabiliser. Pour cela les directions informatiques peuvent rédiger une charte ayant valeur contraignante, précisant les droits et les responsabilités de chacun.

> Plus l'entreprise va s'ouvrir, plus l'éducation des employés au risque sera importante [...] il est de notre devoir d'éduquer nos clients sur la façon de protéger leurs données, les chiffrer... Les DSI ont aussi le devoir de placer des garde-fous. Il faut mettre en place des mécanismes pour détecter si quelqu'un se met à collecter et copier toutes les données à sa portée dans l'entreprise, et bloquer des comportements qui n'ont pas lieu d'être tant à l'intérieur de l'entreprise qu'à l'extérieur. Cela nécessite une éducation des employés mais aussi des clients de l'entreprise.
>
> Yves EYCHENNE, Cloud Advisor, IBM France

REGARD D'EXPERT

Quelle stratégie pour maitriser le Shadow IT ?

— Par Jean Philippe Guillemin

Le problème *«Shadow IT»* a une origine principalement comportementale, ce qui nous conduit généralement à postuler que la sensibilisation des utilisateurs, ainsi que le renforcement de la visibilité/surveillance pourraient se révéler particulièrement efficaces pour limiter les risques associés au phénomène. Considérons que ce sont les deux premiers axes d'une stratégie de maitrise du du Shadow IT, mais cela ne semble pas suffisant.

En effet, n'oublions pas le mouvement technico-sociologique de fond : la digitalisation. On peut effectivement se poser la question suivante: s'il semble possible d'infléchir la tendance comportementale des utilisateurs via la pédagogiene devrait-on pas considérer l'éparpillement généralisé des données comme un mouvement inéluctable ?

En outre, que craint-on principalement du Shadow IT ? Les analyses de risque font remonter de façon récurrente le risque de divulgation de données sensibles. On peut donc considérer que le principal risque associé au Shadow IT concerne la confidentialité des données, même s'il ne faut pas, bien entendu, écarter l'intégrité ainsi que les vulnérabilités induites.

De ce point de vue, on voit apparaitre le troisième volet d'une possible stratégie de maitrise des risques du Shadow IT. Puisque les données sont éparpillées (à la fois pour de bonnes raisons - accessibilité, efficacité, nomadisme, et à la fois pour de mauvaises raisons - Shadow IT), ne devrait-on pas déplacer la sécurité au niveau des données elles-mêmes, afin que les données distribuées embarquent systématiquement le mécanisme de protection avec elles ?

Le troisième axe de notre stratégie dépasse donc le simple problème du Shadow IT. Il est naturellement lié à l'entropie généralisée des données. Il consiste à chiffres les fichiers sensibles de façon obligatoire, et à mettre en oeuvre les nécéssaires systèmes de contrôle d'accès orientés «rôles» et mécanismes de recouvrement des clés.

Bibliographie

- CNIL, BYOD : quelles sont les bonnes pratiques ? Février 2015
- DSIH, Qu'est-ce qu'un CASB ? août 2017
- Globbsecurity, Prévention du Shadow IT : 5 cas d'utilisation d'une solution CASB, février 2018
- Globbsecurity.fr, Rêver d'un monde sans Shadow IT, c'est bien ; s'en assurer, c'est mieux, février 2018
- Juniper, CXP Groupe, l'usage du cloud hybride en France, juin 2016
- Solutions numériques, Le CASB, le chien de garde des accès aux services cloud, octobre 2016
- Solutions numériques, Shadow IT : Le DSI peut-il reprendre le contrôle ? septembre 2016
- Wisper.io, Lumière sur le shadow IT ! juillet 2017

APIXIT

L'expertise augmentée

Ce Livre Blanc est un document d'information rédigé par la société APIXIT.
Il n'a pas vocation à servir de support de prestation de conseil.

SIEGE SOCIAL

Les Conquérants
Immeuble Annapurna
1 avenue de l'Atlantique
91940 LES ULIS

RENNES

Espace Jacques Cartier
CS 96031
35360 MONTAUBAN
DE BRETAGNE

LILLE

Village Créatif
10 rue de la Cense
59650 VILLENEUVE D'ASCQ

QUIMPER

3 allée Emile Le Page
29000 QUIMPER

PARIS

Immeuble AXIUM
22/24 rue du Gouverneur
Général Félix Eboué
92130 ISSY LES MOULINEAUX

NANTES

Les Espaces Océane
4 rue Jack London
44400 REZÉ

REIMS

13 rue Desbureaux
51100 REIMS

TOULOUSE

32 rue des Cosmonautes
31400 TOULOUSE

LYON

Immeuble Woodclub
97, allée Alexandre Borodine
69800 SAINT-PRIEST

5D chemin du Jubin
69570 DARDILLY

www.apixit.fr