DOSSIER D'EXPERTS

PRÉVENTION ET SÉCURITÉ

Cybersécurité et collectivités territoriales

Comprendre les enjeux pour agir

David Assou
Responsable commercial spécialisé cybersécurité

Corinne Czens
Avocate - Responsable de pôle - RGPD - TIC et PI

territorial éditions

Cybersécurité et collectivités territoriales

Comprendre les enjeux pour agir

Les cyberattaques touchant les collectivités territoriales françaises ont augmenté de 50 % de 2019 à 2020. Le phénomène est mondial et son coût global est estimé à plus de 6 000 milliards de dollars.

La mission de la cybersécurité est la protection des systèmes informatiques, numériques et de leurs données à l'aide de moyens techniques, conceptuels, humains ou législatifs. Cette protection vise plusieurs objectifs, mais il s'agit notamment d'assurer l'intégrité, la confidentialité et la disponibilité des données.

Cet enjeu est vital et stratégique pour les collectivités territoriales et concerne aussi bien les communes, les départements, les régions que les établissements publics locaux. Du fait de la transformation digitale que connaissent les collectivités, les nombreux services publics locaux essentiels au bon fonctionnement des territoires sont menacés par une cybercriminalité grandissante qui s'attaque aux vulnérabilités des systèmes d'information.

Proposant une approche intelligible de la cybersécurité - qui est un domaine abstrait, complexe et fragmenté en spécialités techniques - en combinant points de vue opérationnels et juridiques, cet ouvrage s'adresse aux élus responsables de l'attribution des budgets, aux fonctionnaires territoriaux en charge directement ou indirectement de la sécurité du système d'information et, plus globalement, à tous les agents territoriaux, puisque chacun peut devenir un vecteur d'intrusion potentiel.

David Assou est responsable commercial spécialisé cybersécurité dans un grand groupe leader du numérique, dans lequel il a également occupé des fonctions relatives à l'intégration de la cybersécurité dans les projets. Ancien officier supérieur de l'armée de terre, il enseigne la cyberdéfense à l'académie militaire de Saint-Cyr Coëtquidan.

Forte de plusieurs détachements en entreprise ou en entité publique, **Corinne Czens** a une vision pratique du droit. Ancien DPO du Samusocial de Paris, elle intervient en tant que responsable de pôle d'un cabinet d'avocats parisien dans les domaines du droit des contrats, du droit de la protection des données, de la propriété intellectuelle et des TIC.

boutique.territorial.fr

ISSN : 1623-8869 – ISBN : 978-2-8186-1918-6

territorial éditions

DOSSIER D'EXPERTS

PRÉVENTION ET SÉCURITÉ

Cybersécurité et collectivités territoriales

Comprendre les enjeux pour agir

David Assou
Responsable commercial spécialisé cybersécurité

Corinne Czens
Avocate - Responsable de pôle - RGPD - TIC et PI

territorial éditions

CS 70215 - 38501 Voiron Cedex - Tél.: 04 76 65 87 17 - Référence DE 901A
Retrouvez tous nos ouvrages sur boutique.territorial.fr

Vous souhaitez être informé de la prochaine actualisation de cet ouvrage ?

C'est simple !

Il vous suffit d'**envoyer un mail** nous le demandant à :

jessica.ott@territorial.fr

Au moment de la sortie de la nouvelle édition de l'ouvrage, nous vous ferons une **offre commerciale préférentielle.**

Avertissement de l'éditeur :
La lecture de cet ouvrage ne peut en aucun cas dispenser le lecteur de recourir à un professionnel du droit.

ISBN : 978-2-8186-1918-6
ISBN version numérique : 978-2-8186-1919-3
Imprimé par Reprotechnic, à Bourgoin-Jallieu (38) - Février 2022
Dépôt légal à parution

Sommaire

Annexes

Préface

Les collectivités territoriales sont des cibles de plus en plus prisées des cyberattaquants : 30 % des collectivités territoriales déclarent avoir subi une cyberattaque en 2020 (source : villesdefrance.fr). Cette même année, des collectivités de toutes tailles ont été touchées : la Région Grand-Est, le Département d'Eure-et-Loir, la métropole Aix-Marseille-Provence, l'agglomération de La Rochelle, la commune de Bondy ou encore celle de Saint-Paul-en-Jarez, pour ne citer que ces quelques exemples.

La cybercriminalité peut se manifester de différentes manières : demande de rançon, paralysie du système d'information, collecte illégale de données… Le phénomène est mondial. Prise dans sa globalité, la cybercriminalité est estimée à plus de 6 000 milliards de dollars (en détournements de données, demandes de rançons, etc.), soit 6 % du PIB mondial détourné.

Le risque cyber représente donc un réel enjeu pour les entités publiques, dans la mesure où les collectivités se tournent de plus en plus vers le numérique pour leurs activités quotidiennes, d'autant que la crise sanitaire n'a fait qu'accélérer ce phénomène avec la mise en place du télétravail pour beaucoup d'agents territoriaux. Cette digitalisation a considérablement augmenté la vulnérabilité des collectivités territoriales de toutes tailles.

Les collectivités se doivent de protéger leur système contre ces attaques au titre notamment du règlement général sur la protection des données (RGPD), mais également au titre des impacts économiques qu'elles entraînent. En cas de manquement au règlement évoqué, des sanctions pénales peuvent en effet être ordonnées. À ces sanctions s'ajoutent d'importants coûts liés à l'attaque et à la restauration des données : on parle ici de plusieurs centaines de milliers d'euros. Par ailleurs, les enjeux tels que les budgets dédiés à la cybersécurité, la mutualisation des moyens et des ressources ou encore la sensibilisation des acteurs font de plus en plus l'objet d'attention de la part des décideurs locaux.

David ASSOU pour la partie opérationnelle et Corinne CZENS pour les questions juridiques développent tout au long de ce dossier d'experts une approche globale de la prise en compte de la cybersécurité par les collectivités territoriales de plus en plus touchées par les cyberattaques. Les élus, en tant que décideurs, mais également l'ensemble des agents territoriaux œuvrant dans le cadre du service public local, sont concernés par les menaces cyber.

Le constat remonté par les élus est que la littérature relative au domaine de la cybersécurité reste aujourd'hui très technique, fragmentée en de nombreux sous-domaines ou bien traitée de manière parcellaire. Or, si l'objectif est aujourd'hui de sensibiliser et

d'acculturer le plus grand nombre, le domaine de la cybersécurité exige d'être traité de bout en bout et de manière intelligible pour une meilleure compréhension permettant des actions plus efficaces.

Quelles sont les cybermenaces qui visent les collectivités territoriales aujourd'hui ? Comment les collectivités peuvent-elles anticiper ces menaces et comment réagir lorsqu'une cyberattaque se déclare ? Telle est la trame de ce dossier.

Les forces de sécurité intérieure se mettent en ordre de bataille pour faire face à la montée de la cybercriminalité. Créé en février dernier, le commandement de la gendarmerie dans le cyberespace, le ComCyberGend, est entré en fonction en août 2021 pour rassembler sous une même bannière l'ensemble des forces cyber de la gendarmerie. Il s'appuie sur un réseau de 7 000 cyberenquêteurs qualifiés situés sur tout le territoire et assistés de 200 réservistes. La cible de 10 000 cyberenquêteurs est prévue pour fin 2023.

Au travers du ComCyberGend, la gendarmerie amplifie son caractère de force de proximité numérique qui s'adresse à tous les acteurs, notamment les collectivités territoriales, avec lesquelles les gendarmes échangent déjà au quotidien.

Le ministre de l'Intérieur vient par exemple de signer une convention tripartite avec la gendarmerie nationale, cybermalveillance.gouv.fr, et l'Association des maires de France afin de proposer aux adhérents de cette dernière un dispositif d'autoévaluation dénommé « Immunité cyber ». Agissant sous les trois volets de la proximité numérique, de l'investigation et de la recherche, le ComCyberGend vulgarise une matière à la fois grisante pour les progrès qu'elle génère, et menaçante tant elle semble être difficilement contrôlable. Cet ouvrage apportera certainement des réponses aux questions des élus et fera, à n'en pas douter, prendre conscience aux particuliers, chefs d'entreprise et toute personne qui le lira, de l'importance de comprendre la donne cyber et d'y prêter toute l'attention nécessaire.

Général de division Marc BOGET
Commandant de la gendarmerie dans le cyberespace

Partie 1

Les collectivités territoriales face aux cybermenaces

Chapitre I

Une transformation numérique propice aux cyberattaques

A - De la direction des services informatiques à la direction du système d'information

1. La refonte de la relation de service usagers-collectivités

Depuis une quinzaine d'années, la relation dans le cadre du service public local entre les collectivités et les usagers a été bouleversée. Tout d'abord, avec le fort développement d'Internet et du numérique. Après le web statique, on a vu apparaître le web social (réseaux sociaux), le web sémantique (mobilité, géolocalisation, besoin utilisateur) et le web intelligent (apprentissage, automatique, intelligence artificielle). On comptait 3 millions de sites Internet en 2002, 1,8 milliard en 2019. La plupart des collectivités délivrent des services via des sites Internet qui sont fortement exposés sur le web.

Les attentes des usagers sont de plus en plus fortes en la matière. On ne conçoit plus l'utilisation du papier pour faire ses démarches administratives de proximité.

De la même façon, les agents des collectivités ont connu ces dernières années des transformations organisationnelles fortes engendrées par le numérique et les innovations informatiques. La dématérialisation des procédures en est un exemple significatif.

C'est toute une approche du parcours usager dans le cadre des démarches administratives qui a évolué et qui continue de faire gagner en qualité de service rendu par les agents et en vitesse d'exécution.

Les ordinateurs fixes ou portables, les serveurs, les infrastructures de tous types, les applications se sont donc multipliés, créant ainsi de nombreuses possibilités d'innovation, mais également des ***failles**** et des ***vulnérabilités**** propices à la ***cybercriminalité**** [1]. Chaque collectivité, de taille et de compétences différentes, a organisé la sécurité de son système d'information en fonction de son contexte, avec des moyens alloués, selon des priorités décidées démocratiquement, conformément à la clause de compétence générale.

1. L'étoile correspond à une explication/définition donnée à la fin de l'ouvrage.

Par ailleurs, dans le cadre de la mutualisation des compétences au sein de collectivités de même nature, des mutualisations se sont opérées par le biais de la transformation informatique et digitale.

Transformation numérique : collectivités, unissez-vous ! – Extrait

« Parmi les organisations institutionnelles, les collectivités territoriales sont bien entendu très concernées, et notamment les quelque 25 000 communes de moins de 1 000 habitants. Afin de les aider à intégrer l'outil informatique en vue d'offrir le meilleur service à leurs habitants, des structures territoriales d'accompagnement ont vu le jour dès les années 90, sous forme de syndicats informatiques intercommunaux. Dotées de compétences élargies à l'ensemble des usages numériques depuis les années 2000, ces structures sont connues aujourd'hui sous le nom d'« opérateurs publics de services numériques » (OPSN). […] Les projets de transformation numérique des collectivités se multiplient. Ceci amène les métiers des OPSN à évoluer et leurs missions à se renforcer. La première mission de ces opérateurs est la mutualisation des coûts et des moyens. Dans un contexte de contraintes budgétaires fortes sur les collectivités, le numérique est souvent perçu comme un centre de coût important, mais on peut également le considérer comme une source d'économie et un outil d'efficience opérationnelle. Équipements informatiques, licences logiciels, formations des agents, les OPSN assurent un accompagnement de proximité de leurs collectivités membres dans leurs missions quotidiennes.

Lors d'une enquête réalisée au 1er semestre 2020 par l'association Déclic auprès d'un panel de près de 1 800 collectivités répondantes, 70 % d'entre elles confirment que leur OPSN leur permet de réaliser des économies. Il a également été démontré auprès des adhérents d'un OPSN du Val-de-Marne, que ces derniers avaient en moyenne un budget système d'information (SI) inférieur de 25 % à celui d'une collectivité non membre. »

Source : A. Buthion, Banque des territoires, Caisse des dépôts. En ligne : https://www.caisse-desdepots.fr/blog/article/transformation-numerique-collectivites-unissez-vous

2. Le rôle de la direction des systèmes d'information

Le mouvement de transformation digitale de l'administration locale s'est aussi traduit au niveau des collectivités territoriales par un mouvement de réorganisation des services informatiques et de leurs missions.

En effet, nous sommes passés d'une direction, équipe ou responsable informatiques orientés support usagers (l'usager étant principalement l'agent territorial, mais également les élus locaux) à une dimension plus orientée numérique au sens large incluant : la transformation digitale des services au profit des agents, directions et services de la collectivité et des citoyens dans le cadre de leurs différentes démarches administratives.

La DSI d'une collectivité tend donc à se trouver à l'interface entre les services et les agents et poursuit, dans ce contexte, son rôle de conseil et d'assistance auprès des directions métiers qui, confrontées à la numérisation de leurs processus internes, s'appuient de plus en plus sur elle.

Les missions de la DSI consistent à élaborer une politique informatique et une politique de la transformation numérique en définissant un schéma directeur, des moyens financiers, techniques et humains, tout en garantissant la fiabilité et la sécurité du système d'information.

Il s'agit également de mettre en place la transition numérique et superviser la mise en œuvre informatique par des choix d'équipements (matériels, logiciels, réseaux) et des actions de veille technologique.

De plus, le rôle de la DSI consiste à définir et gérer des budgets, planifier et contrôler l'ensemble des projets, superviser les relations avec les partenaires et prestataires exté-

rieurs, à veiller au respect des cahiers des charges, des délais et des budgets. Un autre objectif important de la DSI est de maintenir en conditions opérationnelles les systèmes d'information.

Un changement de culture accompagné – Extrait
[Ville et CA de Beauvais, Oise, 53 communes, 1 800 agents, 103 800 habitants]
« La direction des systèmes d'information et de télécommunication (DSIT) est née de la fusion des services informatiques de la ville de Beauvais (infrastructures et réseau, et services liés aux postes de travail et logiciels) et de l'agglomération. « Nous ne sommes pas structurés pour porter des projets stratégiques, mais tout ce qui a trait au numérique doit passer par nous », précise Nicolas Schockaert, le directeur des systèmes d'information et de télécommunication.
Cette implication du service dans tous les projets n'est pas toujours bien identifiée par les directions. « Lorsqu'un service envisage, par exemple, un partenariat avec une start-up, nous devons y être impliqués, illustre-t-il. C'est un changement de culture que nous accompagnons par une communication régulière. J'assure annuellement, pour y parvenir, une revue des besoins de chaque direction. »
La DSIT impulse également des projets tels que la gestion électronique des documents pour structurer le stockage administratif de la collectivité. « L'idée n'est pas de remplacer les dossiers de stockage sur le réseau mais d'avoir une autre forme de stockage au travers d'une plateforme intranet. Elle embarque aussi des processus qui permettent de mettre en place des formulaires de circulation de signatures. » Pour muscler son service « développement logiciel », la collectivité est, de facto, restreinte par un principe de réalité budgétaire. Et ce, même si c'est la compétence sur laquelle la collectivité a une forte attente. »
Source : J. Krassovsky, « Les DSI plus que jamais au centre du jeu », *La Gazette des communes*, mars 2019. En ligne : https://www.lagazettedescommunes.com/608465/les-dsi-plus-que-jamais-au-centre-du-jeu/

3. La donnée : un enjeu crucial

Alors que les analystes prédisent un triplement du nombre d'objets connectés dans le monde entre 2018 et 2025 pour atteindre 40 milliards[2], la dématérialisation des procédures administratives se poursuit à un rythme soutenu. Ces deux facteurs amènent à la constitution d'un volume important de données publiques, que les collectivités ont pour responsabilité de protéger, et de valoriser. Ces données ont en particulier un rôle à jouer pour adapter en permanence l'action publique, et la rendre plus efficace.

La donnée est devenue progressivement une infrastructure essentielle détenant une valeur, tant du point de vue de la proximité avec les usagers que du point de vue du pilotage des politiques publiques, qu'il convient de considérer à part entière dans la stratégie numérique du territoire, au service de l'ensemble des politiques sectorielles.[3]

Les politiques publiques locales s'analysent, se planifient et s'évaluent avec des cartes, des tableaux de bord croisant des informations en provenance de différents acteurs, pour nourrir les plans stratégiques et sectoriels territoriaux d'éléments factuels d'analyse. Chacune des démarches d'élaboration de ces plans nécessite de disposer d'une vision

2. Source : *Le digital représenterait une économie de 23 000 milliards de dollars à l'horizon 2025,* WIS, l'école de l'expertise digitale. En ligne : https://www.wis-ecoles.com/digital-en-2025/#:~:text=40%20milliards%20d'objets%20connect%C3%A9s,devrait%20logiquement%20s'estomper%20progressivement
3. *Étude sur le cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales,* FNCCR, mars 2019. En ligne : https://www.territoire-numerique.org/wp-content/uploads/2019/04/FNCCR-Etude-cycle-de-la-donnée-v29032019_version-définitive.pdf

précise du territoire et des dynamiques qui y sont à l'œuvre, la disponibilité et la qualité des données sont des enjeux essentiels pour assurer la pertinence des orientations retenues et l'adaptation des programmes aux besoins des usagers.

La première exigence concernant la gestion des données pour les collectivités territoriales est de maîtriser son patrimoine en matière de données. Pour cela, il s'agit de cartographier les données clés disponibles, à l'aune de la stratégie du territoire. Les partenaires internes et externes sont mobilisés pour identifier et partager les données nécessaires à l'élaboration et au pilotage des politiques. Le patrimoine constitué par les données est évalué, pour définir une trajectoire stratégique d'évolution.

Dans le cadre de la mise en cohérence de la stratégie territoriale de la donnée avec les enjeux du territoire, une programmation est également de mise dans le cadre de la transformation numérique territoriale. L'article 1425-2 du Code général des collectivités territoriales prévoit la définition de stratégies de développement des usages et services numériques, en lien avec les schémas directeurs territoriaux d'aménagement numérique. Ces stratégies visent à équilibrer l'offre de services numériques sur le territoire ainsi qu'à favoriser la mise en place de ressources mutualisées, publiques et privées, y compris en matière de médiation numérique.[4]

L'open data dans les petites et moyennes collectivités – Extrait

« Avec la loi pour une République numérique de 2016, la France a été pionnière dans l'adoption d'une stratégie globale d'open data des pouvoirs publics. Ainsi, depuis octobre 2018, les collectivités de plus de 3 500 habitants (ou comptant plus de 50 agents), ainsi que les entreprises délégataires de service public, sont tenues d'ouvrir leurs données. Si les métropoles se sont rapidement saisies du sujet, les petites et moyennes collectivités ont elles aussi des bénéfices à retirer de l'open data. Leurs données sont moins importantes en volume.

En octobre 2020, l'ensemble des régions françaises, 60 % des départements et plus de la moitié des collectivités territoriales comptant plus de 100 000 habitants avaient publié au moins un jeu de données ouvertes. En d'autres termes, des données qui peuvent être consultées, partagées ou exploitées par tout citoyen, acteur économique ou association qui s'en saisit. Cette démarche n'est pas obligatoire pour les plus petites collectivités. Pourtant, certaines d'entre elles se sont aussi mobilisées et ont enclenché une démarche d'open data. » Source : *L'open data dans les petites et moyennes collectivités*, Abylon. En ligne : https://abylon-conseil.com/lopen-data-dans-les-petites-et-moyennes-collectivites/

Qualification juridique de la donnée

Selon le dictionnaire *Larousse*, une donnée se définit notamment par une *« représentation conventionnelle d'une information en vue de son traitement informatique »*.

Selon les définitions listées en annexe 1 de l'arrêté du 22 décembre 1981 sur l'enrichissement de la langue française, le terme « donnée » constitue *« la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement »*.

En droit, la donnée sera appréhendée en fonction du corpus de règles que l'on souhaite lui appliquer : le règlement général relatif à la protection des données à caractère personnel, les règles relatives à la protection du secret des affaires, la protection relative aux bases de données, etc. Chaque corpus comporte des règles permettant de délimiter leur champ d'application, dont parfois une définition précise des données couvertes.

4. https://www.territoire-numerique.org/wp-content/uploads/2019/04/FNCCR-Etude-cycle-de-la-donn%C3%A9e-v29032019_version-d%C3%A9finitive.pdf

	Définition légale	Source
Données informatiques	Une représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système d'information exécute une fonction.	Article 2 de la directive (UE) 2013/40 relative aux attaques contre les systèmes d'information
Données	Les données autres que les données à caractère personnel au sens de l'article 4, point 1, du règlement (UE) 2016/679.	Article 3-1 du règlement (UE) 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »).	Article 4-1 RGPD
Information	Est protégée au titre du secret des affaires toute information répondant aux critères suivants : 1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ; 2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; 3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret.	Article L.151-1 du Code de commerce
Base de données	Un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen.	Article L.112-3 alinéa 2 du Code de la propriété intellectuelle

Parmi les données protégeables, les données à caractère personnel sont celles qui représentent actuellement le plus d'enjeu : big data, intelligence artificielle, vente de fichiers de données et degré de maîtrise de chaque personne sur les données la concernant sont des sujets qui dépassent aujourd'hui largement l'enjeu purement juridique et sont devenus de véritables enjeux économiques et même de souveraineté.

Plus particulièrement, la vision classique des États européens s'oppose à la vision des États-Unis : une vision personnaliste de la donnée *versus* une vision marchande de la donnée.

La donnée se trouve sur une ligne de crête entre la personne, dont la donnée serait l'émanation et protégée en tant que telle au même titre que la personne elle-même, et la chose, donc la donnée en tant qu'objet détachable et détachée de la personne et, à ce titre, en particulier : vendable.

Dans la vision personnaliste, il est impensable que la donnée soit commercialisable et le règlement général sur la protection des données [règlement (UE) 2016/697] est entièrement basé sur cette approche : l'enjeu est de redonner à la personne concernée la maîtrise sur ses données et d'assurer un niveau de protection très élevé des données en vue, notamment, d'augmenter la confiance des consommateurs dans l'économie numérique sur le territoire de l'Union européenne ; la question de leur vente ou cession en contrepartie d'un prix ou de la gratuité d'un service n'est pas directement abordée.

À l'inverse, l'approche qui prédomine aux États-Unis d'Amérique du Nord est fondée sur l'idée selon laquelle le libre accès aux informations et données, y compris dans la sphère privée, par les entreprises est favorable à leur développement. Protéger la vie privée et donc limiter cet accès revient dans cette vision à brider inutilement le développement économique des entreprises.

Ainsi, sur le plan juridique, il n'existe pas de réglementation générale visant à protéger les données. L'autorégulation des acteurs privés, par la mise en place des bonnes pratiques, prédomine et l'État n'intervient que ponctuellement en légiférant sur des points précis, par exemple au sujet de la protection de l'enfance.

Compte tenu de l'augmentation considérable des flux de données transfrontaliers et en particulier vers les États-Unis, les difficultés issues de cette opposition de vision augmentent et sont à la source d'un grand nombre de complexifications juridiques de ces échanges.

B - L'augmentation de la surface d'exposition du système d'information

1. L'extension de la surface d'attaque logique ou informatique

Une surface d'attaque représente l'ensemble des éléments ou des actifs qui peuvent être attaqués pour provoquer un incident de sécurité. Ces actifs sont dits « exposés ».

Alors que la frontière entre ce qui se trouve à l'intérieur du ***pare-feu**** et à l'extérieur est de moins en moins perceptible, il faut considérer aujourd'hui que la surface d'attaque d'une collectivité (tout ce qu'elle doit se préoccuper de défendre) comprend désormais l'intérieur du réseau de la collectivité et s'étend jusqu'aux limites extérieures de l'Internet, et même jusqu'au domicile des agents.

Les chercheurs définissent le terme « exposé » comme une situation dans laquelle n'importe qui peut se connecter s'il découvre les services, y compris les services à distance et dans le cloud. Il est toutefois probable que, la plupart du temps, les organisations ne soient pas conscientes que ces services sont exposés.

La surface d'attaque d'un système d'information comprend par exemple les services web, le réseau, les protocoles de communication ou bien encore les noms de domaine. L'exposition de téléservices sur le web accroît les risques de ***vulnérabilité****. Les téléservices en question peuvent être par exemple : les formalités de paiement en ligne pour la cantine scolaire, de prises de rendez-vous, de démarches d'urbanisme, certificat de domicile, médiathèque, marchés publics, personnes âgées, petite enfance, inscription aux stages multisports.

Pour appréhender sa surface d'attaque, la direction des systèmes d'information doit cartographier les domaines et sous-domaines, serveurs, services exposés et applications ainsi que les accès physiques au système d'information.

Bien appréhender la surface d'attaque permet de mieux gérer et évaluer les risques associés. Différents outils et moteurs de recherche existent pour faciliter cette cartographie : vérifier quels appareils de votre réseau sont accessibles depuis Internet (serveurs, routeurs, imprimantes…), tandis que d'autres outils permettent de trouver les certificats liés à un domaine.

Le ***shadow IT**** doit également être pris en compte pour rendre la cartographie exhaustive. Il s'agit des parties cachées du système d'information non connues de la DSI, un appareil connecté au réseau sans autorisation par exemple.