STORMSHIELD

CYBERSÉCURITÉ DES COLLECTIVITÉS

Un enjeu qui n'attend pas la **smart city**

www.stormshield.com

Cybersécurité des collectivités

Les services publics n'échappent pas à la révolution numérique. Depuis vingt ans, la numérisation des infrastructures collectives et de la vie publique, sous l'effet de l'urbanisation massive et l'explosion des technologies de l'information, étend la surface d'attaque des collectivités et les expose à de forts enjeux de cybersécurité.

Cette période a vu naître le concept de « ville intelligente » ou de « territoire intelligent », rendu plus efficient par de nouvelles technologies dont un véritable écosystème d'objets connectés. Le tout au service d'une meilleure qualité de vie et d'une meilleure gestion des ressources (élément crucial dans la lutte contre le réchauffement climatique).

Si le terme « smart city » décrivait au départ un imaginaire plutôt techniciste, l'expression a évolué avec le temps pour englober des aspects juridiques, écologiques, etc. Technoville, écoville ou autre ; quelle que soit la réalité derrière ce mot-valise, les enjeux cyber sont au cœur de chaque expérimentation.

Smart ou non, les villes, les intercommunalités, les métropoles, les départements et les régions sont particulièrement exposés aux risques de cybersécurité alors qu'elles cumulent les responsabilités. Ce livre blanc présente les défis que rencontrent les collectivités dans la sécurisation de leur numérisation, les solutions et perspectives pour qu'elles puissent demain continuer d'assurer leur mission d'utilité publique. Sans perdre de vue leur devoir de protéger leurs administrés et leurs données.

un enjeu qui n'attend pas la smart city

INTERVENANTS

Yann ARIZA

RSSI de la Communauté de communes de la Vallée du Garon

« Ce sont surtout les ressources humaines dont nous manquons. Nous aurions besoin de plus de personnes au niveau intercommunal pour couvrir l'ensemble des besoins. La réponse est souvent d'externaliser mais cela pose des problématiques de pilotage et de gouvernance. »

P. 38-39
Collectivités et smart cities : comment accompagner le mouvement vers la numérisation ?

Rodolphe de BEAUFORT

Délégué Général Adjoint Gimelec

« Nous accompagnons la pénétration du véhicule électrique. Cela implique par exemple d'équiper près de 250 000 bâtiments résidentiels collectifs avec parking en infrastructures de recharge (IRVE) d'ici 2035 ou 2040. »

P. 56
Quel avenir pour le concept de smart city ?

Noël CHAZOTTE

Product Manager Stormshield

« Les solutions de sécurité existent, notre défi est de les adapter à ces environnements et à la diversité des types de connexion réseau. »

P. 16
Les dessous du risque cyber des collectivités

Sébastien DAGOT

Ingénieur commercial Stormshield

« Dans le cas d'attaques ciblées, l'objectif peut être de couper l'accès à un service ou d'empêcher la collectivité de communiquer avec ses administrés. »

P. 21
Pourquoi les collectivités intéressent-elles les cyber-criminels ?

Jérôme NOTIN

Directeur Général Cybermalveillance.gouv.fr

« Nous observons que près de 20 % des répondants ne sait pas dire comment est gérée la sécurité informatique de la collectivité. Plus préoccupant encore : 8 % des sondés déclarent n'assurer aucune gestion de sécurité informatique. »

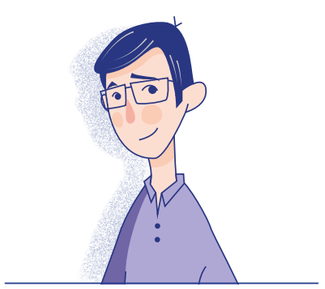
P. 24
Interview exclusive sur les principaux enseignements de l'enquête sur les collectivités

Vincent NICAISE

Industrial Partnership and Ecosystem Manager Stormshield

« La reprise en main par de grandes villes de leurs infrastructures critiques implique le recrutement de profils cyber spécialistes des réseaux industriels et de leurs automates. »

P. 49
Un cadre règlementaire qui se muscle



Joël RIVALLAN

Président ASTEE Bretagne Pays de la Loire

« Le secteur de l'eau, habitué à des investissements importants pour améliorer ses réseaux, devrait avoir les moyens d'investir dans du matériel plus évolué pour se mettre à niveau en matière de cybersécurité. »

P.51
Cybersécurité des collectivités, tout n'est pas (qu') une question d'argent

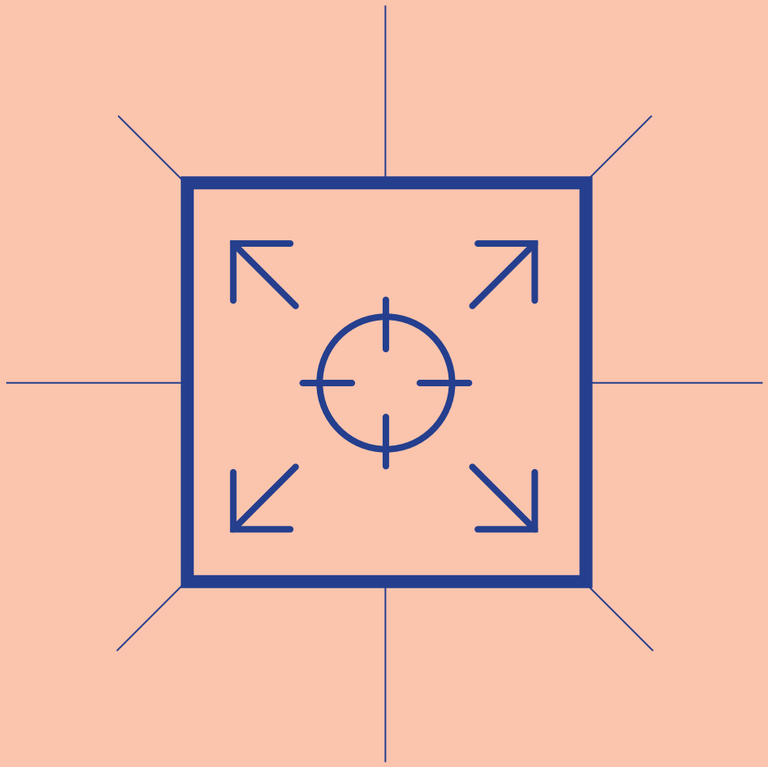
Témoignage ANONYME

DSI d'une ville française de plus de 150 000 habitants

« Nous avons élaboré une fiche cyber qui est désormais remplie à chaque démarrage de projet pour identifier les enjeux et le niveau de sécurité à exiger de la part des prestataires en fonction de la criticité du projet. »

P. 40
Comment suivre les recommandations des autorités compétentes ?

SOMMAIRE



Collectivités & smart city :

une histoire de surface d'attaque

Que ce soit pour fluidifier leur relation aux citoyens, faciliter l'intervention de leurs agents ou encore optimiser leurs processus et consommations en tout genre, les villes se numérisent. Ce qui les rend plus vulnérables aux incidents informatiques et ouvre de nouvelles opportunités aux cyber-criminels.

01

La numérisation des collectivités, entre ouverture et défis cyber

La notion de « smart city » fait écho au choix d'une commune, d'une ville, d'une métropole, d'un département ou d'une région d'interconnecter tout ou partie de ses systèmes pour créer de nouveaux services. Quels risques ces interconnexions émergentes et complexes font-elles courir aux collectivités ?

La plupart des services techniques de mairie sont informés de la défaillance de leurs équipements. En cas de dysfonctionnement d'un lampadaire par exemple, les habitants peuvent le faire remonter directement. Dans une collectivité qui a numérisé la gestion de son éclairage public par exemple, ou une smart city, ce lampadaire connecté signale lui-même la panne via un dispositif d'IIoT. Un algorithme de maintenance prédictive aurait également pu déclencher une intervention avant même qu'elle ne se produise. Le même principe d'infrastructures communicantes peut s'appliquer aux bennes de collecte de verre, à la gestion des parkings, des places de piscine, etc.

Cette infrastructure numérique enrichit les services et téléservices, développe de nouvelles fonctionnalités, optimise les consommations. Mais ces interconnexions entre systèmes informatiques classiques (IT) et systèmes opérationnels (OT) contribuent également à créer un environnement plus complexe et donc plus délicat à protéger. Celui-ci expose les collectivités et les smart cities à de nouvelles vulnérabilités en plus de les mettre au défi de l'interopérabilité.

IIoT - INDUSTRIAL INTERNET OF THINGS

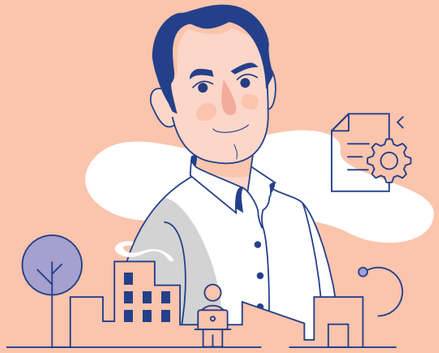
En définitive, toutes les collectivités sont amenées à s'appuyer sur les nouvelles technologies pour adresser les grands enjeux de la ville de demain. Et même si l'ampleur de la numérisation de leurs activités varie énormément en fonction de leurs ambitions et de leurs moyens, la sécurisation de cette transition représente, elle, un défi commun.

DANS "TERRITOIRES" CONNECTÉS, IL Y A IIOT

L'Industrial Internet of Things désigne les capteurs intelligents qui permettent de connecter des éléments physiques, comme des lampadaires ou des valves de réseau d'eau, à Internet. Ce faisant, il devient possible d'échanger avec eux des données qui viennent alimenter des solutions logicielles.

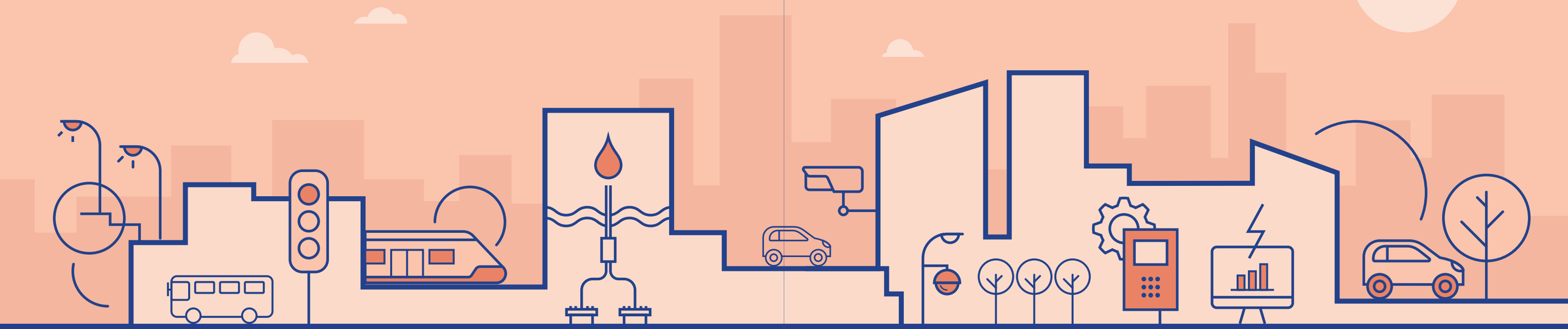
L'offre de téléservices aux citoyens et citoyennes est géré par la métropole dont nous dépendons. En revanche, nous mettons à disposition des différentes directions métiers de la ville et de leurs agents des services qui permettent d'optimiser la gestion opérationnelle. Pour cela, nous travaillons au préalable ***sur l'interconnexion sécurisée entre leurs réseaux (informatiques comme industriels) et le SI.***

DSI d'une ville française de plus de 150 000 habitants



Projections sur la ville connectée **et les risques cyber associés**

En connectant ses systèmes essentiels, la smart city offre de nouvelles perspectives mais étend du même coup sa surface d'attaque. Série d'exemples de risques cyber auxquels elle s'expose.



Éclairage

Plonger un quartier dans le noir en piratant le système d'éclairage

Signalisation

Perturber le trafic automobile en désynchronisant les feux de signalisation

Mobilité urbaine

Désorganiser les transports publics en s'introduisant dans le système de gestion de la circulation

Eaux

Polluer en arrêtant une pompe de relevage pour que toutes les eaux soient rejetées dans une rivière

Vidéosurveillance

Surveiller illégalement des individus en détournant l'usage des caméras

Gestion technique

Désactiver la sécurité incendie en pénétrant le système de Gestion Technique du Bâtiment

Énergie

Couper l'électricité dans un bâtiment public

Parking

Perturber la tarification dynamique du stationnement

Les enjeux décryptés
avec **Rodolphe de Beaufort**,
Délégué Général Adjoint au
sein de Gimelec

En marche vers la smart city ?

Il y a maintenant près de 15 ans, l'univers des systèmes urbains s'est rapproché de celui de l'informatique et des nouvelles technologies. De cette rencontre est né le concept de smart city. Il a bien mûri depuis.

Si beaucoup ont rêvé au départ d'une sorte de tableau de bord unique, les différentes expérimentations ont mis en évidence la difficulté d'unifier tous les systèmes de pilotage en une plateforme unique.

Après cette phase de maturation ces dernières années, nous revenons aujourd'hui à une approche de la ville connectée plus pragmatique, un peu moins ambitieuse en termes d'interconnexion. Les acteurs de la smart city se concentrent désormais sur des cas d'usage précis afin d'être capable de valoriser la récolte de données.

La smart city a ainsi été redécoupée en plus petits silos. L'objectif : intégrer les technologies informatiques dans les domaines OT de façon adaptée à chaque métier. Le concept est donc moins monolithique qu'avant, en Europe du moins, où nous devons composer avec l'existant.

Les dessous du risque cyber des collectivités

Avec une surface d'attaque étendue, les collectivités en pleine numérisation sont exposées à la malveillance de cyber-criminels. Leurs vulnérabilités peuvent désormais être exploitées pour atteindre des infrastructures opérationnelles, avec des conséquences potentielles dramatiques.

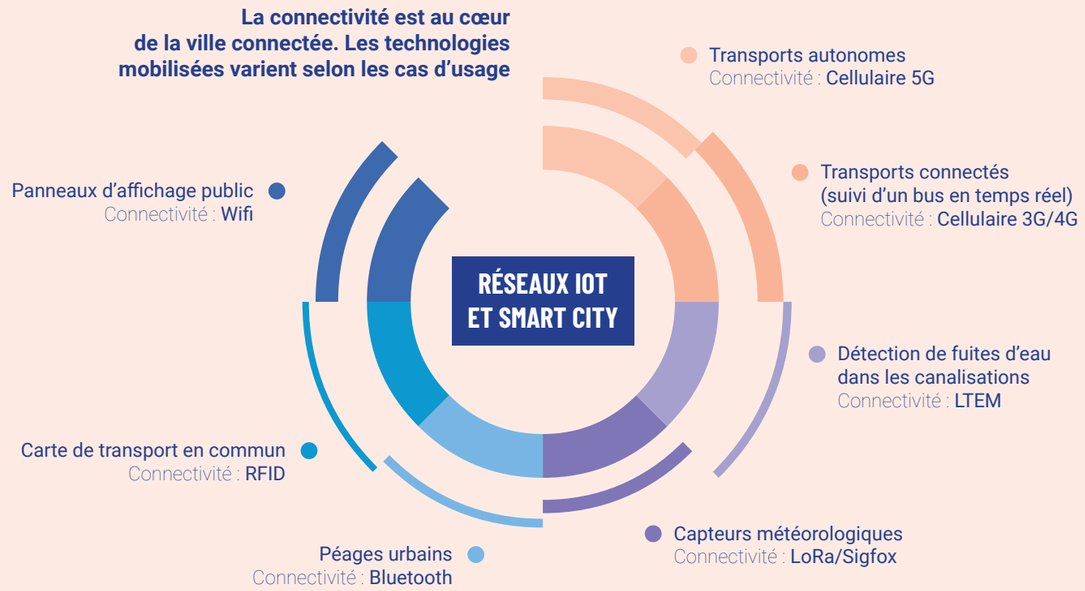
En observant de plus près, les raisons de la fragilité numérique des collectivités peuvent être attribuées à quatre facteurs :

- **L'interconnectivité des systèmes**
- **La maintenance à distance**
- **La présence dans l'espace public**
- **La pluralité des acteurs**

L'INTERCONNECTIVITÉ DES SYSTÈMES

Des capteurs sur la chaussée comptabilisent les véhicules. Cette information, issue des réseaux industriels, alimente le système de gestion des feux routiers. Désormais, elle peut également être transmise depuis les capteurs vers les réseaux informatiques, voire Internet, à une application de gestion du trafic. Autant de données dont l'intégrité doit être assurée lors de la collecte, du stockage et du traitement.

La mise à disposition des données comme ici avec data.grandlyon renforce leur poids dans l'action publique : en plus d'orienter les décisions, elles deviennent un outil de communication.



***Les solutions de sécurité existent**, notre défi est de prendre en compte l'évolution de ces environnements et la diversité des types de connexion réseau.*

Noël Chazotte,
Product Manager Stormshield

LA MAINTENANCE À DISTANCE

En particulier pendant et depuis la période COVID, l'enjeu est de sécuriser de nouveaux usages de maintenance à distance. La démocratisation des accès à distance via des VPN réduit les déplacements, par exemple sur les sites des réseaux d'eau souvent très éloignés sur le territoire. Mais elle crée aussi de nouvelles portes d'entrée dans l'infrastructure.

LA PRÉSENCE DANS L'ESPACE PUBLIC

Les équipements de systèmes urbains sont également plus susceptibles d'être vandalisés car plus accessibles que des baies informatiques sécurisées en intérieur.

LA PLURALITÉ DES ACTEURS

Les opérations à distance ajoutent de nouveaux acteurs au nombre déjà important d'intervenants sur les réseaux industriels des villes : propriétaire, délégataire et sous-traitants doivent se conformer aux meilleures pratiques cyber.

Cette situation peut conduire à des attaques, des dysfonctionnements et même des pannes, au retentissement majeur (blackout, perte de contrôle, perturbations diverses, perte de données, effets de panique). Elle peut également être exploitée par des cyber-criminels (manipulation et paralysie de l'infrastructure urbaine, attaque en déni de service, diffusion de fausses informations, fraude, etc.).

À cela s'ajoute les capacités de cybersécurité limitées des systèmes industriels. En effet, il s'avère difficile de maintenir en condition de sécurité un parc hétérogène et/ou non évolutif. La fiabilité des différents types de connectivité sans fil pose également question (authentification mutuelle, chiffrement, continuité d'activité).

CHIFFRE CLÉ

1 COLLECTIVITÉ SUR 3

déclare avoir un faible niveau de protection cyber, dans l'étude 2023 de Cybermalveillance.gouv.fr

Les **incidents et cyberattaques contre des collectivités** à travers le monde

Aux quatre coins du monde, aucune collectivité n'est épargnée par la menace cyber. Ce phénomène mondial place la sécurité des données des citoyens au cœur des préoccupations des collectivités territoriales.

Tour d'horizon - non exhaustif - des cyberattaques à l'échelle mondiale.

Première cyberattaque reconnue contre une smart city à Olsztyn (Pologne)

Olsztyn est une smart city polonaise, située à 200 km au nord de Varsovie. Le 24 juin 2023, sa régie de transports a subi une attaque de ransomware qui a engendré de nombreux embouteillages et perturbé l'achat de tickets dans les transports publics. Heureusement, la signalisation a continué à fonctionner en mode dégradé.

Smart ou pas, grandes ou petites, pourquoi les collectivités intéressent-elles les cyber-criminels ?

Quel que soit leur stade de numérisation, les collectivités font l'objet d'attaques à répétition. Comment ces opérations malveillantes évoluent-elles dans le temps ? Qui est à la manœuvre ? Quelles sont les motivations de cette filière criminelle ?

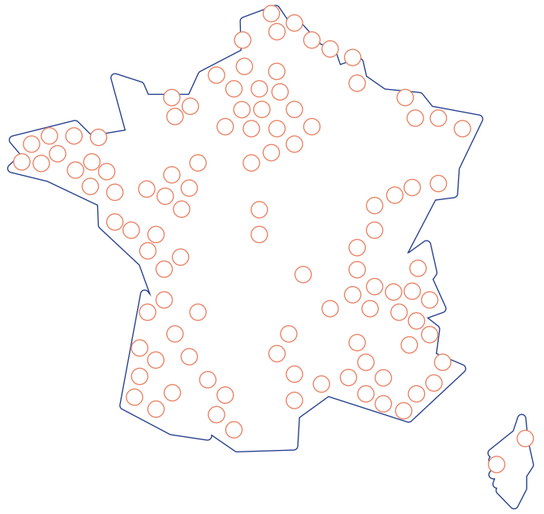
Nombre de collectivités font l'objet d'attaques opportunistes voire sont simplement victimes collatérales d'attaques de grande ampleur. C'est ce qui est généralement observé dans le cas des ransomwares : **les collectivités ne sont pas visées spécifiquement mais elles font partie des milliers de cibles attaquées.**

Néanmoins, les institutions publiques sont soumises à de forts enjeux de sécurité, de continuité de service et d'image. Elles peuvent donc parfois être prises pour cible en raison des nuisances qu'entraînent l'arrêt de leurs activités. Enfin, les données personnelles et sensibles traitées par le secteur public peuvent constituer une manne financière non négligeable pour les cyberattaquants qui réussiraient à les obtenir : la photo utilisée pour un document officiel comme une carte d'identité délivrée par la mairie peut ainsi valoir entre 2 et 5 euros. Un dossier médical, obtenu en s'introduisant dans le SI d'un établissement de santé dépendant d'une collectivité, entre 50 et 250 euros.

*Dans le cas d'attaques ciblées, **l'objectif peut être de couper l'accès à un service ou d'empêcher la collectivité de communiquer avec ses administrés**. Les modes opératoires sont comparables à ce que subissent les entreprises privées mais attaquer le service public s'apparente parfois à un acte politique en allant à l'encontre de l'intérêt du citoyen*

Sébastien Dagot,
Ingénieur commercial Stormshield

Les collectivités locales et hôpitaux publics touchés par des cyberattaques



L'association Déclic, qui réunit les structures de mutualisation informatique à savoir les opérateurs publics de services numériques (OPSN), recense dans cette carte toutes les collectivités locales, intercommunalités, syndicats, hôpitaux publics, régies et Services d'incendies et de secours (SDIS) victimes d'actes de cybermalveillance depuis 2019.

Certaines (rares) attaques contre des administrations publiques émanent d'ailleurs d'acteurs étatiques et participent d'une volonté d'affaiblissement géopolitique voire d'actes de guerre (comme l'attaque contre le réseau énergie ukrainien en 2015).

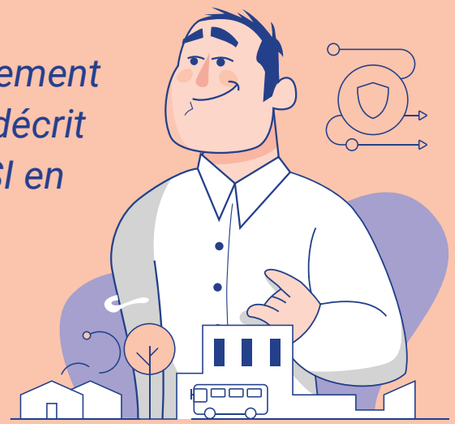
Orléans (2020), Aix-Marseille-Provence (2020), Châlon-sur-Saône (2021), Frontignan (2022) ou encore Caen (2022) ; Lille (2023), Morlaix (2023), Chantilly (2023) mais aussi Mandeure (2023), et Beton (2023) ; aucune collectivité ne semble à l'abri. **Quels que soient sa taille et son degré de numérisation, toutes sont concernées par la question cyber.**

C'est ce qui a poussé le Groupement d'intérêt public (GIP) ACYMA d'ouvrir en 2017 la plateforme Cybermalveillance.gouv.fr. Son objectif : sensibiliser les collectivités, les petites et moyennes entreprises et les particuliers à la question cyber en France. Le dispositif mène des actions de sensibilisation, dont la dernière, fin 2023 est un baromètre dédié à la cybersécurité des collectivités de moins de 25 000 habitants.

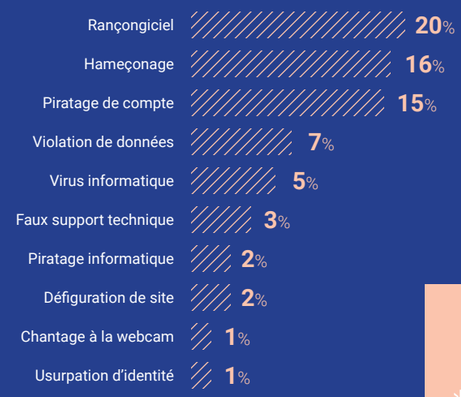
La modernisation des infrastructures et des équipements des collectivités s'accélère avec la numérisation de la société et des services publics. **Cette course à l'innovation des villes connectées se fait parfois au détriment de la sécurité et profite à la filière criminelle.** Dès lors, comment accompagner ce mouvement vers plus d'interconnexion en toute cybersécurité ?

*Il nous est arrivé deux fois de détecter des **tentatives d'intrusion de ransomware**. Heureusement, nous avons pu, dans les deux cas, procéder à une remédiation directe. Cela dit, cette menace fait peur. Au-delà des conséquences techniques, j'ai été particulièrement marqué **par l'impact humain** décrit dans les témoignages de RSSI en ayant fait les frais.*

Yann Ariza, RSSI,
Communauté de communes de la vallée du Garon



PRINCIPALES RECHERCHES D'ASSISTANCE SUR LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR



CHIFFRE CLÉ

1 COLLECTIVITÉ SUR 10

déclare avoir déjà été victime d'une ou plusieurs attaques au cours des 12 derniers mois, dans l'étude 2023 de Cybermalveillance.gouv.fr

INTERVIEW EXCLUSIVE

Jérôme Notin, Cybermalveillance.gouv.fr

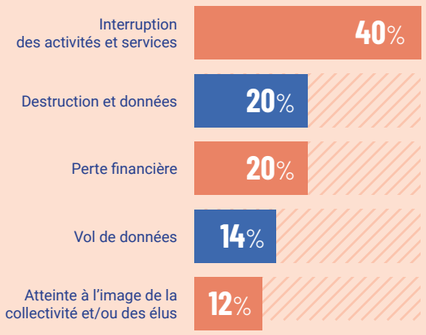
Enquête sur la cybersécurité des collectivités : les enseignements à retenir

« *Seules les cyberattaques sur les grandes collectivités font l'actualité pourtant, elles sont toutes concernées* ». C'est le premier constat que dresse le Directeur Général du dispositif national d'assistance aux victimes de cybermalveillance.

La question de la maturité face aux risques

Un second constat concerne la perception du risque, puisque 20 % des collectivités interrogées ne savent pas évaluer leur niveau d'exposition face aux cyberattaques. Un chiffre qui traduit peut-être un manque de maturité sur le sujet. « *Néanmoins, la conscience du risque progresse avec 33 % des collectivités sensibilisées en 2021 contre 78 % en 2023. Une sur trois l'a d'ailleurs été de façon régulière.* » Car les conséquences qui en découlent sont tout aussi dramatiques pour les collectivités, comme leurs administrés.

Principales conséquences des cyberattaques des collectivités



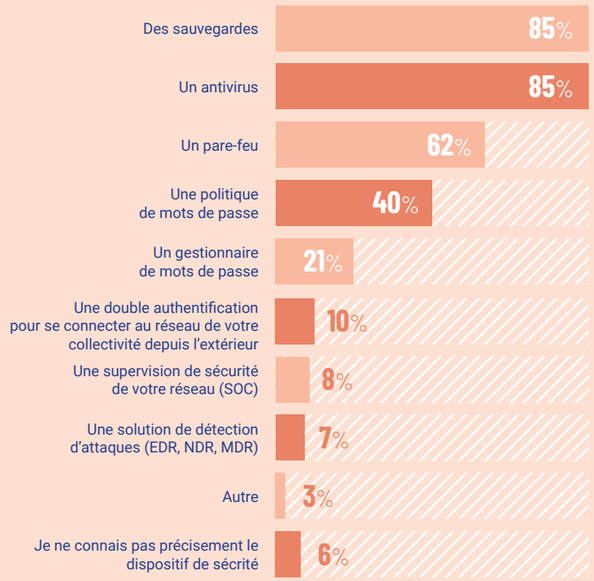
INTERVIEW EXCLUSIVE

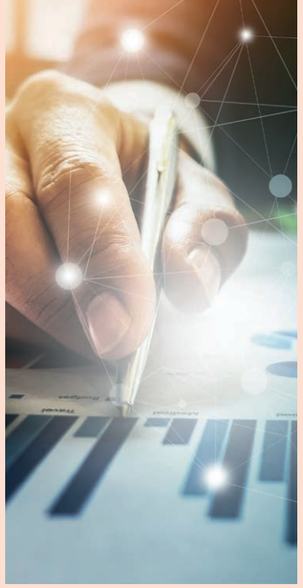
Nous observons que près de 20 % des répondants ne sait pas dire comment est gérée la sécurité informatique de la collectivité. Plus préoccupant encore : ***8 % des sondés déclarent n'assurer aucune gestion de sécurité informatique.***

La question de l'équipement cyber

J.N. *La majorité des collectivités compte trois dispositifs de sécurité en moyenne, sauvegarde, antivirus et firewall en tête. Cette situation explique sans doute qu'une collectivité sur deux se sent bien protégée – souvent à tort…*

L'équipement des collectivités en matière de dispositifs de sécurité





La question des budgets

J.N. *Malgré des perceptions plutôt favorables, nous constatons que les moyens alloués à la cybersécurité sont limités. 65 % des collectivités interrogées disposent de moins de 5 000 euros de budget informatique annuel et 75 % disposent d'un budget cyber inférieur à 2 000 euros. Parmi elles, seules 12 % prévoient une évolution à la hausse pour l'année à venir.*

Ce manque de moyens entraîne des usages à risque : une collectivité sur deux ne fournit ni tablette ni téléphone par exemple, ce qui conduit 88 % des répondants à utiliser leur téléphone portable personnel à des fins professionnelles. Un risque accru pour les collectivités, d'autant plus quand les collaborateurs doivent également utiliser leurs clés USB et ordinateurs personnels.

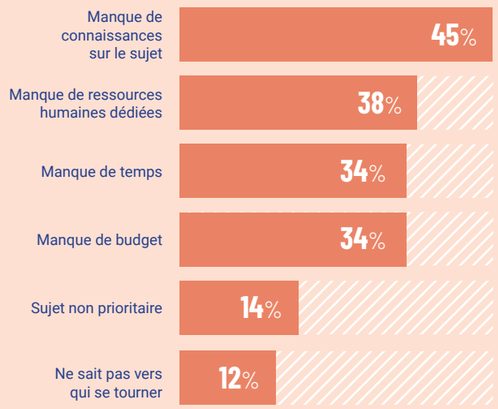
La question des freins

J.N. *Pourtant, à la question de ce qui freine la cybersécurité des collectivités, le budget n'arrive qu'en troisième position, à égalité avec le manque de temps.*

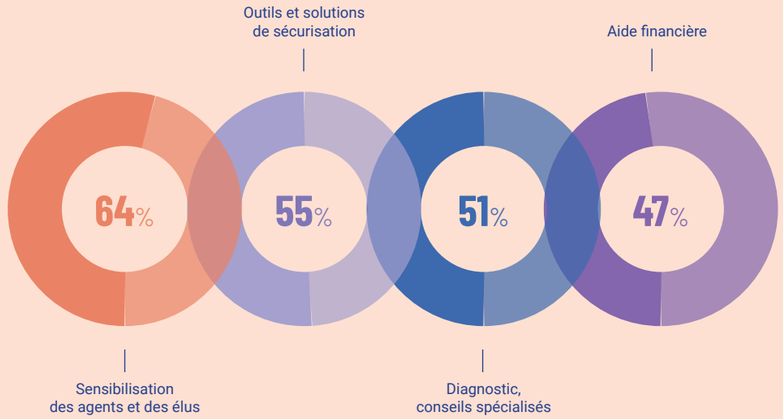
Le fait que le manque de connaissances soit le plus cité (45 %) nous conforte dans l'idée que nos actions de sensibilisation constituent un vrai levier. Bien sûr, il y a toujours une minorité de sondés qui jugent que le sujet n'est pas prioritaire (14 %) mais 64 % des personnes interrogées évoquent la sensibilisation comme besoin numéro un.

Nous notons une réelle prise de conscience, mais elle doit s'étendre à toutes les populations au sein des collectivités et s'accompagner de mesures concrètes pour que les réflexes cyber s'installent durablement. Le recours à des produits de sécurité qualifiés par l'ANSSI et quelques bonnes pratiques permettent déjà de faire un bond en matière de sécurisation informatique.

Les principaux freins cyber des collectivités



Besoins prioritaires des collectivités en cybersécurité



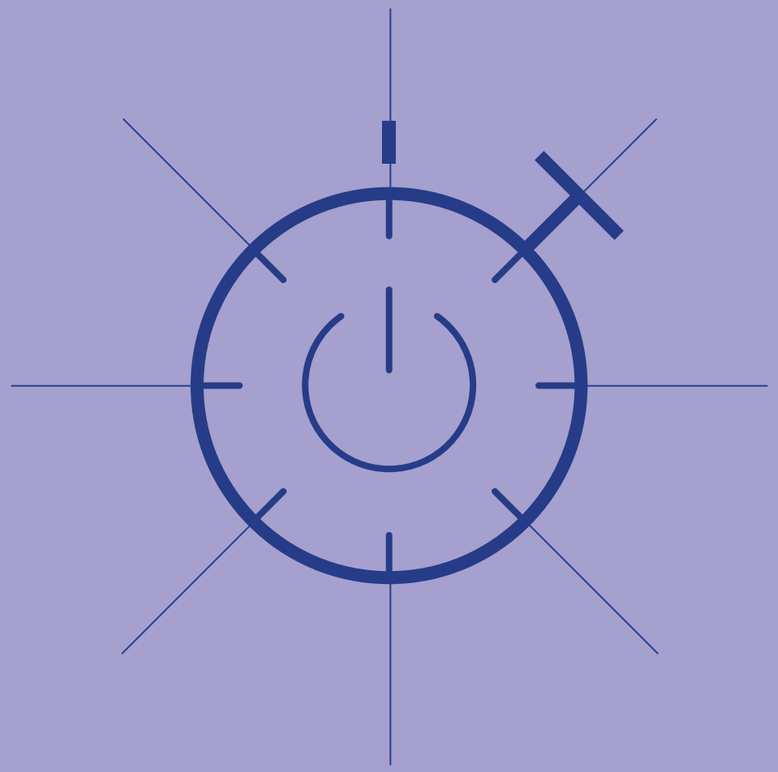
La question des besoins

J.N. *Notre étude place les outils et solutions, les conseils ainsi que la sensibilisation comme les attentes les plus fortes de la part des collectivités. Des besoins en priorité sur les volets techniques et humains ; un résultat qui témoigne d'une certaine prise de conscience des enjeux.*

Prise de conscience qui, si elle évolue positivement, doit toucher toutes les populations des collectivités, et ce régulièrement pour que des réflexes s'instaurent durablement et qu'elles puissent être armées face aux cyberattaques.

Retrouvez l'étude en intégralité ici

SOMMAIRE



Collectivités & smart city :

comment accompagner le mouvement vers la numérisation ?

Alors que les villes composent
avec des incertitudes croissantes
aux niveaux social, économique et climatique,
une certitude demeure : tôt ou tard,
elles feront l'objet d'une cyberattaque.
Dans ce paysage urbain toujours plus
numérique, par où commencer
la mise en cybersécurité des collectivités ?

02

En faisant travailler ensemble des acteurs hétérogènes

Les environnements des collectivités et encore plus de la smart city se caractérisent par un millefeuille d'intervenants, ce qui n'est pas sans poser problème. Ce foisonnement multiplie les interconnexions à sécuriser et peut conduire à une dilution de la responsabilité cyber.

Dans le cadre d'un appel d'offres dédié à la collectivité connectée, l'agglomération émettrice expose par exemple son souhait de connecter un équipement de voirie avec une plateforme de maintenance. **Cette demande suppose que différents acteurs s'associent pour répondre : un opérateur télécom qui va fournir la carte SIM intégrée au capteur IoT, un installateur, une société de maintenance, un éditeur logiciel, un hébergeur, etc.** Parmi tous ces acteurs, qui intègre la cybersécurité ? Qui est responsable de la confidentialité, de l'intégrité et la disponibilité des données ? Celui à qui elles appartiennent ? Celui qui les collecte ? Qui les traite ? Les agrège ? Tout le monde ? Personne ? Difficile d'y répondre tant chaque cas est différent.

Ce flou n'est pas réservé aux prestations externes car rares sont les collectivités à bénéficier d'une gouvernance claire et transversale en matière de cybersécurité.

> *De grandes différences de maturité cyber persistent entre les grands exploitants nationaux de réseaux d'eau, soumis à la directive NIS et disposant de services spécialisés, et les structures moyennes comme les régies qui exploitent elles-mêmes leurs installations.*
>
> Joël Rivallan,
> Président ASTEE
> Bretagne-Pays de la Loire

> *De nombreux cas d'usage ne sont pas déployés car l'organisation des collectivités est elle-même trop 'silotée'. Sans management global de nos systèmes urbains, le partage d'informations et la diffusion de bonnes pratiques sont rendus complexes.*
>
> Rodolphe de Beaufort,
> Délégué Général Adjoint,
> Gimelec

Le constat n'est pas meilleur dans les plus petites communes. Si la gouvernance cyber y est simplifiée, le facteur humain prend une dimension tout autre car bien souvent, une seule personne gère toute la chaine de validation. « *Dans les plus petites communes, nous signons juste un flux et non plus des factures. Nous sommes donc moins vigilants* », reconnaissait Sylvain Le Chatton, Maire de Liancourt-Saint-Pierre (60) et Vice-président de la communauté de communes du Vexin Thelle (France), à propos des nouveaux processus d'achat et de règlement numérisés lors d'une table ronde organisée par Cybermalveillance.gouv.fr. L'élu rapportait également les tentatives d'arnaques au faux support subies par sa secrétaire de mairie. Il confiait enfin ne pas toujours savoir vers qui se tourner face à la profusion d'acteurs : un appel à fusionner certains dispositifs ?

Ces situations plurielles rendent difficile l'application d'une méthode universelle. Pourtant, en France toutes les mairies portent les mêmes responsabilités et les mêmes engagements de service public, quelle que soit leur taille.

Focus sur les acteurs de la cybersécurité des collectivités et de la smart city

Élus et administrations des collectivités : municipalité ou intercommunalité (métropole, communauté de communes)

Leur rôle ? Décider des politiques publiques et des investissements.

Intégrateurs

Leur rôle ? Assurer l'intégration de la solution de sécurité dans l'environnement de production.

Opérateurs réseaux

Leur rôle ? Gérer l'installation et l'exploitation des réseaux de télécommunications, des systèmes de sécurité informatique et des moyens téléphoniques.

Éditeurs de logiciels

Leur rôle ? Créer et développer des solutions informatiques.

Fabricants

Leur rôle ? Fabriquer les éléments matériels qui composent les solutions utilisées (capteurs IoT par exemple).

Opérateurs publics de services numériques (OPSN)

Leur rôle ? Accompagner les collectivités en fournissant des prestations informatiques et de cybersécurité.

Délégataires de services publics

Leur rôle ? Ces acteurs privés ont la délégation par contrat de la gestion d'un service public.

Exploitants

Leur rôle ? Cette entité opère une infrastructure (ex : réseau d'eau), une collectivité en direct ou un tiers par concession ou délégation de service public.

Centrale d'achat

Leur rôle ? Sélectionner des prestataires de cybersécurité de confiance.

En déployant des solutions de cybersécurité adéquates

Faut-il se résigner à débrancher les collectivités connectées ? À revenir en arrière sur la numérisation des services au citoyen ? Non, car des moyens de protection cyber existent. Et les appliquer aux collectivités, en route ou non vers la smart city, permettrait de continuer à profiter des bénéfices de services publics connectés.

Pour sécuriser les systèmes d'information d'une smart city ou d'une collectivité connectée, il faudrait mettre en place une politique de sécurité globale puis l'adapter à chacun des SI. Et c'est bien souvent là que tout se complique. Car en plus de la pluralité des acteurs, **les collectivités doivent conjuguer les enjeux de différents périmètres de réseaux, IT comme OT.** Des réseaux aux priorités divergentes et aux règles de sécurité différentes.

SUR QUEL LEVIER POUVEZ-VOUS AGIR ?

- Recourir à des solutions de confiance
- Réfléchir à une gouvernance cyber globale
- Cartographier vos différents réseaux et les segmenter
- Mettre en place une identification multifacteur
- Opter pour l'architecture Zero Trust
- Privilégier le Security by Design
- Prendre en compte l'évolutivité du SI et penser aux enjeux et aux utilisations de demain dès maintenant
- Imposer des clauses contractuelles pour établir clairement les domaines de responsabilité

Vous souhaitez approfondir la question et préciser vos leviers d'action ? Nos experts restent à votre écoute.

Pour protéger la collectivité connectée, il ne suffit donc pas de sécuriser les nouveaux usages : c'est bien l'intégralité du SI existant qu'il faut prendre en considération. Au-delà de l'aspect technique et de la mise en place d'outils de sécurisation, les experts en sécurité informatique doivent s'appuyer sur la compétence des maires, des directions générales des services et des directions de la sécurité informatique pour sensibiliser le plus grand nombre d'agents en fonction de leur contexte.

CHIFFRE CLÉ

94% DES COLLECTIVITÉS

interrogées dans l'étude 2023 de Cybermalveillance.gouv.fr sont équipées d'au moins 1 dispositif de cybersécurité, mais seules 62% évoquent le pare-feu, 10% la double authentification, 7% une solution de détection d'attaques.

En suivant les recommandations des autorités compétentes

Pour faciliter le travail de sécurisation, les autorités ont développé un certain nombre de dispositifs d'accompagnement et des ressources qui aider les collectivités dans leur démarche.

En France, l'ANSSI répertorie les dispositifs d'accompagnement à destination des collectivités dans un catalogue en trois volets : **sensibilisation, protection et réponse à incident.** L'autorité française édite également des guides pour diffuser les bonnes pratiques, dans lesquels elle recommande l'utilisation de produits de cybersécurité certifiés. La certification atteste de la robustesse d'un produit de sécurité et indique que son éditeur l'a soumis à un laboratoire indépendant pour la réalisation de tests.

À l'image de ce qui est fait en cas de cambriolage, le dépôt de plainte permet de mobiliser une brigade numérique pour identifier les éléments utiles à l'enquête au plus tôt.

Christophe HUSSON,
Commandant en second
de la Gendarmerie
dans le cyberespace ComCyberGend

Mais les administrations publiques doivent en parallèle se conformer aux réglementations européennes et nationales de cybersécurité telles que le RGPD, le Cybersecurity Act voire la classification de sécurité « Restreint UE » pour l'échelle européenne, et le Référentiel Général de Sécurité (RGS) ou encore la Politique de sécurité des systèmes d'informations de l'État (PSSIE) en France. Dans certaines situations, les collectivités doivent alors faire appel à des solutions de cybersécurité qualifiées. Au-delà de la simple certification, la qualification atteste quant à elle de la confiance accordée par l'État français au dit produit de sécurité.

Outre les solutions techniques et organisationnelles mises en place en amont, la réaction aux incidents se révèle être une clé dans la gestion de crise cyber. Les collectivités françaises ont ainsi l'obligation de déclarer les incidents aux autorités compétentes, à savoir la CNIL et l'ANSSI. Dans le cas d'un incident de sécurité, le dépôt de plainte auprès de la gendarmerie est fortement recommandé.

Quelle est la réalité des collectivités au quotidien ? Quel est leur périmètre ? Quelle organisation se met en place ? Deux profils aux premières loges des questions de cybersécurité au sein des collectivités apportent leur éclairage.

Quelle est la nature et le périmètre de votre mission ?

Yann A. Notre service a été créé en 2018 pour assurer le maintien en condition opérationnelle de quatre infrastructures : celle des communes de Brignais, Chaponost, Millery et celle qui correspond aux besoins propres de la CCVG. Les communes de Montagny et Vourles, bien que faisant partie de la communauté de communes ne bénéficient pas de cette mutualisation de ressources et de compétences.

Nous nous occupons également, le plus possible, du maintien en conditions de sécurité. Mais nous sommes quatre collaborateurs, il est difficile de tout faire. Nous gérons environ 1 400 terminaux (postes, téléphones, tablettes) pour 450 utilisateurs.

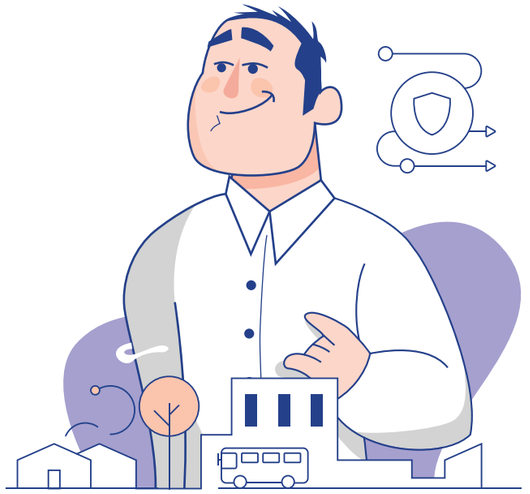
50 km²

+30 000 habitants

200 km de voirie

Solutions cyber déployées

firewalls, EDR, protection des messageries, sauvegarde cloud, PRA/PCA, virtualisation.



Yann Ariza est RSSI de la Communauté de communes de la Vallée du Garon (CCVG), située dans le département du Rhône en France.

Votre communauté de communes propose-t-elle des téléservices ? Qu'avez-vous déployé pour les sécuriser ?

Y.A. Le téléservice le plus important au sein de la CCGV est un portail famille. Il permet de gérer les inscriptions à la cantine ou au périscolaire et de calculer le quotient familial.
Il s'agit d'un logiciel sur étagère car nous n'avions pas de capacité de développement en interne. À l'issue d'un benchmark de différents éditeurs, nous avons choisi l'outil qui correspondait le mieux à notre besoin.

L'hébergement et la sécurisation des données traitées reviennent à l'éditeur mais cette responsabilité est partagée. C'est à nous, collectivités, de le questionner et de passer en revue le contrat pour vérifier les certificats, la conformité RGPD, etc.

Quels freins rencontrez-vous dans la sécurisation des infrastructures informatique et opérationnelle de votre communauté de commune ?

Y.A. La compréhension des enjeux est encore partielle. Les agents des collectivités territoriales réalisent généralement bien l'intérêt de la double authentification en ligne car elle fait écho à leur expérience de particulier, sur le site de leur banque par exemple. Ils la comprennent moins sur les accès distants. Ils ont parfois l'impression que les données publiques ne sont pas sensibles. Il faut donc continuer de les sensibiliser, quel que soit leur niveau hiérarchique pour améliorer la sécurité globale.

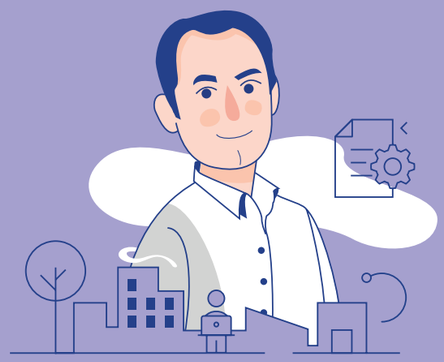
La question des coûts se pose également. Par exemple, les abonnements représentent un poste de dépense de fonctionnement important. Mais avec un budget en augmentation, ce sont surtout les ressources humaines dont nous manquons. Nous aurions besoin de plus de personnes au niveau intercommunal pour couvrir l'ensemble des besoins. La réponse est souvent d'externaliser mais cela pose des problématiques de pilotage et de gouvernance.

Nous réalisons un énorme travail de sensibilisation auprès des directions métiers qui comprennent les enjeux mais pas toujours les implications. Et ça marche !

***Nous avons élaboré une fiche cyber qui est désormais remplie à chaque démarrage de projet pour identifier les enjeux et le niveau de sécurité à exiger de la part des prestataires en fonction de la criticité du projet**.*

La difficulté réside maintenant surtout dans le décalage entre nos exigences cyber et la maturité des fabricants d'IoT et des installateurs. Ils sont encore trop peu formés à ces questions

Témoignage d'un DSI d'une ville de plus de 150 000 habitants.



SOMMAIRE

Collectivités & smart city :

un monde à part, entre considérations administratives et politiques

Les questions administratives et réglementaires revêtent une dimension particulière dans le secteur public. Par définition la politique y tient également un rôle majeur. Au fil des expérimentations, ces aspects dessinent peu à peu les contours éthiques et juridiques de la smart city.

03

Un cadre réglementaire qui se muscle

Au fil des années, le cadre réglementaire dans lequel s'inscrivent les collectivités connectées s'est étoffé. Le but ? Renforcer la confiance des usagers dans les services numériques et encadrer la transformation numérique des États tout en améliorant la sécurité des données à caractère personnel.

La définition d'un cadre réglementaire et juridique entend protéger les SI des collectivités engagées dans une transformation numérique plus ou moins profonde.

En Europe, celui-ci s'articule autour de trois principes fondamentaux que sont **la gouvernance, la gestion des risques et l'amélioration continue,** et vise la sécurisation des interactions, des données et des acteurs critiques.

Retrouvez ce cadre réglementaire expliqué en détail dans le guide ANSSI dédié

Sécuriser les interactions

Tous les téléservices qui mettent en relation les usagers et les autorités administratives doivent répondre aux exigences de sécurité contenues dans le Référentiel général de sécurité (RGS) pour l'administration française. Ce texte définit notamment le processus de qualification des prestataires de services de confiance. Complémentaire, le règlement eIDAS vient lui aussi encadrer les interactions numériques entre le secteur public et les administrés (identification électronique, etc.). Ces deux textes se recoupent parfois, sur la sécurisation de la signature électronique par exemple.

Le réglementaire, parce qu'il accroit le risque juridique, constitue un levier précieux pour augmenter le niveau de cybersécurité global des collectivités.

Yann Ariza,
RSSI de la Communauté de communes de la Vallée du Garon

Sécuriser les données

Une partie des données collectées par les villes connectées constituent des données personnelles. À ce titre, elles sont concernées par le Règlement Général de Protection des Données (RGPD). Certaines collectivités territoriales traitent des données de santé qui doivent faire l'objet de mesures d'hébergement spécifiques, visées par une certification HDS. C'est le cas des départements avec les données des Maisons Départementales pour les Personnes Handicapées (MDPH) ou des communes avec les centres communaux d'action sociale (CCAS). Jean-Michel Morer, Maire de Trilport (77) et représentant de l'Association des Petites Villes de France (APVF) rappelait à ce sujet que « *Dans la gestion du risque, il faut [désormais] intégrer le cloud.* »

Sécuriser les acteurs critiques

En Europe, la directive Network and Information Security (NIS), adoptée le 6 juillet 2016, prévoit des règles de sécurité spécifiques pour les opérateurs de services essentiels (OSE) dont certaines collectivités font partie. Ces entités doivent ainsi identifier les systèmes d'informations essentiels (SIE) et tenir à jour une analyse de risques les concernant. Parmi les autres règles observées, la réalisation à intervalles réguliers, d'audits de sécurité, le cloisonnement de chaque SIE, la protection des accès distants ou encore la mise en place d'un service de traitement des alertes transmises par l'ANSSI.

La nouvelle version de cette directive européenne, baptisée NIS2, a été votée en novembre 2022. Celle-ci est en cours de transposition dans le droit national de chaque pays de l'Union Européenne. Dans le cadre de la transposition en France, l'ANSSI est en lien avec toutes les associations professionnelles des métiers concernés (eau, énergie, santé, etc.) pour adapter la loi aux enjeux de chacun.

NIS2 : vers un élargissement des acteurs concernés en Europe

NIS2 prévoit d'ores et déjà une extension sans précédent du périmètre d'applicabilité. Un nombre conséquent de collectivités va devenir Entité Essentielle ou Entité Importante et les acteurs de leur chaine d'approvisionnement, notamment dans les champs de la gestion des déchets, de l'eau ou du numérique, seront concernés par les mêmes obligations. La nouvelle réglementation prévoit d'ailleurs un mécanisme de sanction renforcé pour garantir l'application du texte.

En parallèle de NIS2, les grandes infrastructures des collectivités françaises (énergie, eau, transports, etc.) sont très souvent qualifiées d'opérateurs d'importance vitale (OIV) et doivent, à ce titre, respecter les obligations de cybersécurité mentionnées dans la Loi de programmation militaire (LPM).

Vigilance de mise

Contrairement à ce que prévoient d'autres textes, les entités soumises à NIS2 ne seront pas notifiées. Charge donc à chaque collectivité d'être proactive et de se renseigner sur son obligation ou non de conformité.

Et les normes métier dans tout ça ? En complément des réglementations cyber pures, certaines réglementations techniques, propres à chaque métier, intègrent un volet cyber. Mais elles font plus figure d'exception que de règle.

Cet ensemble de normes contribue à réduire le risque de sécurité informatique en augmentant le risque juridique en cas de manquement à la protection des données personnelles ou autre.

Vous voulez approfondir la question sur les aspects règlementaires ? Nos experts restent à votre écoute.

> *Dans les métiers de l'eau, peu de textes abordent la question de la cybersécurité. Ils mentionnent bien quelques prescriptions basiques mais pour ce qui est de la sécurisation des dispositifs industriels, c'est vraiment nouveau pour nous et nos référentiels.*
>
> Joël Rivallan,
> Président ASTEE Bretagne
> Pays de la Loire

La place du politique

La cybersécurité des organisations comporte toujours une dimension humaine liée aux compétences et au degré de sensibilisation. Dans le cas des collectivités, cet aspect est renforcé par le poids du politique : il définit les priorités mais le temps du mandat électoral n'est pas toujours celui de la cybersécurité.

Évoluer dans le secteur public présente une particularité non négligeable : le cap peut changer au gré des aléas de la vie politique. Aux États-Unis, en Amérique du Sud et en Asie, les équipes municipales sont élues tous les 4 ans, en France, tous les 6 ans. Or, la sensibilité à la cybersécurité varie parfois en fonction des sensibilités et peut interférer dans le niveau de priorité accordé au sujet. Cette dépendance débouche sur un manque de visibilité qui peut remettre en question la continuité de l'action des experts en cybersécurité.

> *La reprise en main par de grandes villes de leurs infrastructures critiques implique le recrutement de profils cyber spécialistes des réseaux opérationnels et de leurs automates.*
>
> Vincent Nicaise,
> Industrial Partnership and
> Ecosystem Manager Stormshield

> *Généraliser les bonnes pratiques cyber dans les collectivités suppose qu'un engagement politique pérenne soit pris. D'où l'importance de ne pas laisser ces sujets à l'initiative locale.*
>
> Rodolphe de Beaufort,
> Délégué Général Adjoint,
> Gimelec

De la volonté politique dépend également le choix d'internaliser ou d'externaliser les compétences. En 2020, en France, la Métropole de Lyon a ainsi décidé de reprendre la gestion de la production et de la distribution d'eau potable. Cette décision signifie qu'elle a désormais la responsabilité de la sécurisation de l'alimentation en eau mais aussi celle de la cybersécurité des réseaux opérationnels et informatiques impliqués dans le processus.

À l'autre bout du spectre, 57 % des responsables informatiques dans des collectivités de moins de 3 500 habitants déclaraient en 2021 ne pas être formés à la sécurité numérique. La mutualisation des compétences entre plusieurs collectivités, comme le fait la CCVG et comme le recommande le Sénat français, apparaît dans ce contexte comme une solution plus abordable que l'intervention en prestation d'un RSSI dans chaque commune.

Cybersécurité des collectivités : tout n’est pas (qu’) une question d’argent

Si le budget est le nerf de la guerre cyber dans tous les secteurs, les collectivités et administrations ont des processus d’achat bien spécifiques qui contribuent à en faire un univers à part. Dans lequel la collectivité connectée et la smart city doivent s’inscrire.

La cybersécurité de la collectivité connectée est-elle en panne de financements ? Difficile de répondre de façon univoque tant l’hétérogénéité des acteurs décrite p. 26-27 est synonyme d’hétérogénéité de budget.

Malgré tout, la majorité des collectivités consacrerait moins de 10 % de leur budget IT à la cybersécurité, se plaçant en-deçà de la recommandation de l’ANSSI. Dans le cadre du volet cybersécurité du plan France Relance (2020), l’agence s’est vu confier le pilotage d’un fonds de 136 millions d’euros. Des moyens, parfois jugés insuffisants, pour renforcer la sécurité des SI des organismes publics, collectivités territoriales, ministères et établissements de santé.

> *Le secteur de l’eau, habitué à des investissements importants pour améliorer ses réseaux, devrait avoir les moyens d’investir dans du matériel plus évolué pour se mettre à niveau en matière de cybersécurité.*
>
> Joël Rivallan,
> Président ASTEE Bretagne - Pays de la Loire

Le principal frein en matière de cybersécurité des collectivités se situe plutôt au niveau des ressources humaines : elles peinent à embaucher les bons profils. Néanmoins, l'enjeu financier reste présent et il faudra voir comment les pouvoirs publics accompagneront la mise en application des nouvelles exigences de NIS2, notamment dans les petites structures.

Sébastien Dagot,
Ingénieur commercial
Stormshield

Malheureusement, le statu quo n'est pas une option au vu du coût de l'inaction. En février 2021, en France, la ville de Chalon-sur-Saône et l'agglomération du Grand Chalon ont par exemple dû débourser 500 000 € pour remettre leurs systèmes informatiques sur pied après une cyberattaque.

90 000 EUROS

C'est le montant de subvention perçu sur deux ans par la CCVG dans le cadre de France Relance. « *Notre budget informatique augmente : un peu moins de 300 000 euros par an en investissement et en maintenance informatique, auxquels s'ajoutent quelques outils cyber pour environ 20 000 € annuels* », complète Yann Ariza.

Pour les petites communes qui ne disposent pas d'une armée d'acheteurs, passer par une centrale réduit les risques liés au processus d'appel d'offres. Elles s'assurent ainsi d'être juridiquement dans les clous et de voir leurs dépenses validées lors d'un éventuel contrôle de la cour régionale des comptes.

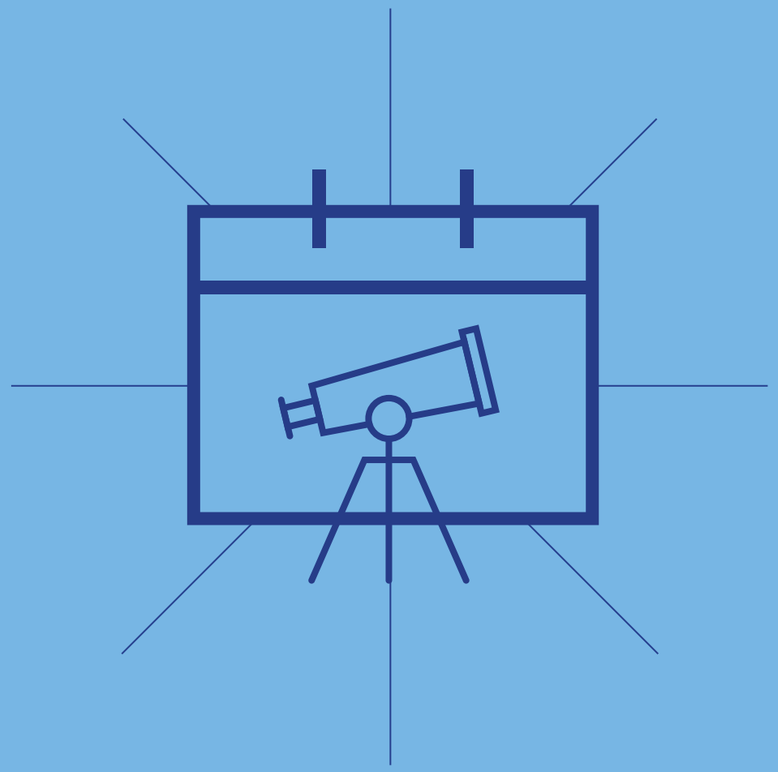
Vincent Nicaise,
Industrial Partnership and
Ecosystem Manager Stormshield

Mais là où le secteur public se distingue plus significativement des organisations privées, c'est dans les mécanismes en place pour dépenser cet argent.

Une collectivité souhaite instaurer un système de paiement numérique des stationnements sur son territoire ? En vertu du code de la commande publique, elle doit organiser un appel d'offres afin d'attribuer le marché, sauf si la valeur de celui-ci la dispense de publicité et de mise en concurrence.

Pour éviter d'avoir à faire elles-mêmes la mise en concurrence et la rédaction de l'appel d'offres, certaines villes et territoires connectés préfèrent passer par une centrale d'achat, comme l'Union des groupements d'achats publics (UGAP). Dans ce cas de figure, c'est la centrale d'achat qui aura réalisé l'appel d'offres en consultant éventuellement des bureaux d'études.

SOMMAIRE



Collectivités & smart city : **et demain ?**

Entre interconnectivité galopante et nouveaux usages, à quoi ressembleront nos villes demain ? Quels seront les ingrédients de leur cybersécurité ? En quinze ans, les représentations autour de la smart city ont évolué, jusqu'à remettre en cause son statut de « modèle » incontournable. Alors demain, des collectivités toutes connectées et sécurisées ?

04

Quel avenir pour le concept de smart city ?

Quels sont les nouveaux usages qui modèleront l'avenir de nos villes ? Poursuivront-elles leur chemin vers l'interconnectivité, se rapprochant d'un idéal de smart city technologique et sécurisée ?

Si les capteurs de pollution ou les trottinettes connectées font déjà partie intégrante du paysage urbain, d'autres applications de la connectivité et de l'Internet des Objets viendront sans doute peupler demain nos villes devenues « smart ».

Ces nouveaux usages émergent dans tous les secteurs : la logistique du dernier kilomètre sera peut-être largement opérée par de petits robots autonomes d'ici quelques années. À condition d'adapter les infrastructures et le cadre juridique.

Le paysage qui se dessine pour les villes du futur ne sera pas le même aux quatre coins du globe. Si en Europe, la tendance est à la conversion lente des villes anciennes, les États-Unis ont pris le raccourci de convertir des quartiers plutôt que des villes entières. Ailleurs dans le monde se créent de vraies villes nouvelles, dans le désert saoudien pour The Line ou dans la province chinoise du Hebei pour la ville-jardin Xiong'an.

POURRA-T-ON UN JOUR PROTÉGER LA SMART CITY ?

OUI

Joël R. *La motivation est là et NIS2 va pousser à s'y mettre !*

Rodolphe dB. *La vraie question est plutôt celle de la stratégie adoptée. Dans l'énergie par exemple, confiera-t-on la question à un acteur national public, au risque de créer une surface d'attaque complète, ou à une multitude d'acteurs privés qui devront tous réaliser des investissements importants.*

NON

Noël C. *La protection à 100% n'existe pas. La puissance et les moyens déployés au niveau étatique sont tellement importants que ces attaques sont difficilement neutralisables… Pour autant, il est possible de se protéger efficacement face à la majorité des autres menaces.*

Yann A. *Nous ne reviendrons pas en arrière sur la connexion et la surface d'attaque donc la sécurisation est nécessaire. Mais elle engage l'intervention de l'État et des investissements conséquents.*

DSI anonyme. *Tant que nous n'aurons pas une normalisation très ferme, chaque installation d'IoT représentera un risque de sécurité supplémentaire. Les enjeux sociétaux sont importants mais la réalité du terrain rend le risque difficile à contrôler.*

INTERVIEW CROISÉE

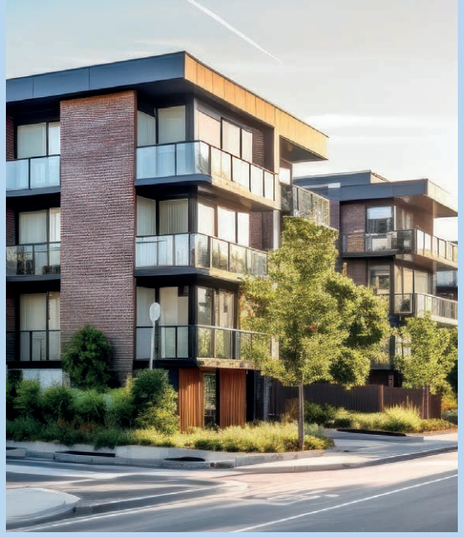
Fenêtre sur demain

Rodolphe de Beaufort et Joël Rivallan donnent des perspectives sur les usages amenés à se développer dans leur métier respectif de l'énergie et de l'eau.

DE L'ÉLECTRICITÉ DANS L'AIR DE LA SMART CITY

R.dB. Nous accompagnons la pénétration du véhicule électrique. Cela implique par exemple d'équiper près de 250 000 bâtiments résidentiels collectifs avec parking en infrastructures de recharge (IRVE) d'ici 2035 ou 2040. L'idée est bien entendu de les connecter à Internet pour en faciliter l'usage. Nous anticipons aussi les problématiques qui surgiront quand les 15 ou 20 millions de véhicules concernés seront raccordés. De même, la généralisation du chauffage électrique, en remplacement d'une partie des systèmes à gaz par des pompes à chaleur, entrainera également l'apparition de nouveaux cas d'usage : ceux-ci seront optimisés par les systèmes de gestion du bâtiment (GTB) qui permettent une flexibilité des consommations et doivent être progressivement déployés dans les bâtiments tertiaires publics et privés d'ici 2027.

> *Nous anticipons les problématiques qui surgiront quand les 15 ou 20 millions de véhicules concernés seront raccordés.*
>
> Rodolphe de Beaufort,
> Délégué Général Adjoint,
> Gimelec



PLUS UNE GOUTTE D'EAU (USÉE) PERDUE

J.R. Jusque récemment la réutilisation des eaux usées était bloquée par la réglementation française. De nouveaux décrets vont nous permettre d'en augmenter les proportions, en parallèle de nos efforts d'hydro économie.

DES SOLUTIONS INTELLIGENTES QUI PASSENT À L'ÉCHELLE

R.dB. Au niveau de la production électrique, les choses vont évoluer également à mesure que les systèmes photovoltaïques vont se répandre. Le pilotage local de l'énergie (microgrid) et l'autoconsommation collective devraient se diffuser par la même occasion.

Quelles solutions techniques et organisationnelles pour la collectivité connectée ?

Sécuriser les usages et les infrastructures des collectivités connectées reposent autant sur des solutions techniques qu'organisationnelles. Entre solutions autonomes et administrables, l'avenir désignera-t-il un vainqueur ?

La décentralisation fait écho au transfert de compétences et de moyens de l'État aux collectivités territoriales. C'est aussi une des caractéristiques techniques de la smart city : un ensemble de capteurs et d'équipements distribués sur tout le territoire concerné. Selon ce principe, les équipes de Stormshield conçoivent une solution de sécurité maillée qui garantit la communication entre les différentes parties prenantes du réseau quel que soit leur point d'accès. Ce qui est particulièrement adapté à la diversité des connexions réseau d'une smart city.

En assurant la protection des données au niveau des couches basses, la solution permet de créer un réseau maillé de tunnels de communication sécurisés entre différents éléments d'un réseau de confiance sans en maîtriser l'infrastructure.

MOT CLÉ

COUCHES BASSES

Expression qui fait référence au modèle Open Systems Interconnection (OSI). Il décompose le processus de communication entre deux éléments du réseau en sept catégories, baptisées « couches ». Les couches basses correspondent aux couches 1 (actifs critiques) et 2 (sécurité des données).

Autre solution technique qui devrait gagner en popularité, le XDR. Derrière ce sigle se cache un nouveau paradigme pour la cybersécurité : l'eXtended Detection & Response permet de gérer via une plateforme unique tous les incidents de sécurité. Cette approche améliore l'efficacité opérationnelle et le niveau de protection des structures qui l'implémentent car, en plus des alertes, elle autorise le pilotage d'éléments de réponse et de remédiation.

Enfin, les équipes de prospective technologique et de R&D imaginent des systèmes de sécurisation plus adaptés aux environnements smart cities et à leurs infrastructures distribuées. Mais l'enjeu de la sécurisation de la smart city et des usages connectés de la ville de demain n'est pas que technique. Au plan de moyens humains, les recrutements sont difficiles car ces environnements nécessitent des expertises qui appartiennent à deux mondes différents, l'IT et l'OT.

Noël Chazotte,
Product Manager
Stormshield

Installer un logiciel de sécurité sur un équipement modeste en taille et en capacité de calcul : c'est le défi qui nous pousse à innover pour nous insérer entre le capteur et le système de collecte. Notre agent Stormshield sera disponible sur les postes de travail et nous souhaitons travailler avec de plus en plus d'industriels pour l'embarquer nativement dans les équipements des environnements OT. Notre but est de retirer l'épine cybersécurité du pied de nos partenaires industriels pour qu'ils puissent se concentrer sur les protocoles métier.

MIROIR

Qui gagnera le match de la cyber des smart cities ?

Scénario 1

LE TRIOMPHE DU PLUG AND PLAY

Les solutions les plus simples et les plus intégrées prennent le dessus car elles nécessitent moins de configuration et de maintenance et par conséquent moins de compétences.

Scénario 2

LA VICTOIRE DE LA CAPACITÉ D'ADMINISTRATION

Le côté « boite noire » de solutions « autonomes » n'est pas compatible avec les exigences de certains contextes opérationnels. Cela amène à développer des interfaces accessibles aux directions métier non expertes via lesquelles elles peuvent réaliser des ajustements.

L'ambition du début de mandat était clairement orientée smart city mais l'empreinte carbone du SI est de plus en plus scrutée. Cela joue dans les décisions prises par les élus.

Yann Ariza, RSSI de la Communauté de communes de la Vallée du Garon

« *La doctrine [cyber des collectivités] est en train de s'écrire* ». C'est la formule employée par Jean-Michel MORER, Maire de Trilport et représentant de l'Association des Petites Villes de France (APVF).

Le dynamisme dans les échanges entre les collectivités à propos de la création d'un label spécifique à la cybersécurité laisse entrevoir une montée en compétence globale à l'œuvre.

Pour poursuivre leur chemin vers la smart city, les collectivités ont besoin d'être soutenues par des volontés politiques durables, assorties de moyens financiers suffisants.

Or, ces dernières années, la question écologique s'invite dans le débat et pousse les élus à réfléchir à l'impact environnemental de tels usages au-delà des bénéfices affichés sur l'optimisation des consommations par exemple.

Sans aboutir forcément à un rejet en bloc de la technologie, ces réflexions modifient la définition même de la ville intelligente et de ses représentations : aujourd'hui, smart veut dire numérique mais aussi et surtout sobre et responsable.

SOURCES

- Interviews
- **Olsztyn-Pologne, première Smart City touchée par une cyberattaque**, lemagit.fr
- **International agencies issue smart city cybersecurity guide**, cities-today.com
- **The smarter, the city, the scarier, the cyber risk**, emergingtechbrew.com
- **Angers ouvre un lieu public pour comprendre sa smart city**, lesechos.fr
- **Smart cities vulnerable to cyberattacks**, independentaustralia.net
- **Les « Smart Cities » sous l'angle du risque cyber**, club-ebios.org
- **Enjeux cybersécurité smart city 1-2**, riskinsight-wavestone.com
- **Dallas spend 4m threat detection after ransomware attack**, statescoop.com
- **Cybersecurite IOT, quelle protection pour la smart city ?**, stormshield.com
- **San Francisco multiplie les projets Smart City dans les transports et le stationnement**, lemagit.fr
- **Cyberattaques, quand les collectivites cherchent la parade**, stormshield.com
- **Ville intelligente, toutes les solutions logicielles qui digitalisent les collectivités**, ugap.fr
- **Catalogue marché public, territoires intelligents**, ugap.fr
- **La cybersecurite parent pauvre des budgets informatiques des collectivites**, banquedesterritoires.fr
- **Cyber attack map,** konbriefing.com
- **Cybermoi/s 2023 :** événement de lancement au Campus Cyber, cybermalveillance.gouv.fr

Cybersécurité des collectivités
Un enjeu qui n'attend pas la smart city

STORMSHIELD
22, rue du Gouverneur Général Eboué
92130 Issy-les-Moulineaux, France

Contenu éditorial : Ultramedia
Direction artistique, maquette, illustrations et mise en page : Studio Orkidées

LE CHOIX EUROPÉEN
DE LA CYBERSÉCURITÉ
www.stormshield.com