Cybersécurité & territoires intelligents

Comment sécuriser les usages numériques des collectivités ?

Edito

La cybersécurité : un socle essentiel pour la dynamique des territoires intelligents

Orange, engagé aux côtés des collectivités dans la dynamique des smart territoires et de la donnée territoriale est aussi un acteur majeur de la cyber-protection des entités publiques de toutes tailles.

De la commune rurale aux régions en passant par les départements, métropoles et villes médianes, les territoires intelligents doivent aujourd'hui intégrer la cybersécurité en tant que brique essentielle au développement de leurs nouveaux usages numériques.

Dans cette perspective, les équipes d'Orange Cyberdefense accompagnent les élus et services pour diagnostiquer, protéger et surveiller leurs systèmes d'information afin de préserver leur patrimoine de données. Pour inventer le territoire de demain tout en sécurisant le fonctionnement de la collectivité et la délivrance des services aux habitants, plus que jamais Orange est à vos côtés.

Hugues Foulon,
Directeur Exécutif Groupe Orange
Président Directeur Général Orange Cyberdefense

Sommaire

Les chiffres clés

99 500

incidents de cybersécurité traités par Orange Cyberdefense en 2022 [soit en moyenne plus d'un incident par jour et par organisation][1] parmi 60 milliards d'événements collectés et analysés dans le monde, chaque jour[4]

+18%

d'entités victimes de cybermalveillance en Europe en 2022[1]

82%

des organisations victimes de cyberextorsion ont un effectif inférieur à 1000 collaborateurs[1]

1er

Les rançongiciels figurent au premier rang des menaces redoutées par les collectivités[2]

2ème

Les collectivités sont, de fait, les organisations les plus touchées par des rançongiciels, juste après les PME et ETI[3]

23%

c'est la part des collectivités dans les incidents déclarés à l'ANSSI en 2022 en lien avec des rançongiciels[3]

66%

des incidents affectant l'administration publique ont une origine interne[1]

Sources : **(1)** Security Navigator Report 2023 – Orange Cyberdefense. **(2)** Etude IDC France / Orange Cyberdefense 2021. **(3)** Panorama de la cybermenace 2022 – Anssi. **(4)** Plaquette Orange Cyberdefense.

La cybersécurité : quels enjeux pour les collectivités ?

L'observation des cybermalveillances à l'encontre des collectivités territoriales au cours des dernières années fait émerger un point de consensus, partagé par tous les analystes : la question n'est pas de savoir « si » la collectivité sera attaquée, mais « quand ». Dans ce contexte, chaque territoire, quelle que soit son échelle, peut gagner à anticiper pour se prémunir des risques de manière structurée.

Protéger
les données de la collectivité et de ses habitants

Intégrité
Confidentialité
Disponibilité

Lien de confiance aux citoyens

Assurer
la continuité des services

Fonctionnement de la collectivité

E-administration & services connectés sur le territoire

Renforcer
son système d'information

Résilience après une attaque ou un incident

Limitation des impacts fonctionnels, financiers et sur l'activité des agents

Enjeux d'image

Cybermalveillance : quelles menaces pour les collectivités ?

De quelles cybermalveillances les collectivités sont-elles victimes ?

Les cyberattaques à l'encontre des collectivités connaissent un essor croissant depuis 2019 et ne cessent d'affecter un nombre grandissant d'entités.
Les modes opératoires des cybercriminels se perfectionnent progressivement au cours de ces dernières années. Tour d'horizon des principales menaces qui pèsent sur les territoires.

Des attaques opportunistes

Hameçonnage avec usurpation d'identité, rançongiciels, défaçage de site internet, détournement de ressources informatiques… les modes opératoires des assaillants sont multiples, les dégâts souvent considérables, y compris en termes d'image.

Dans 80 % des cas, les collectivités sont victimes d'attaques opportunistes, sans qu'elles soient spécifiquement visées en tant qu'entités publiques. Pour autant, le brassage de données sensibles dotées de valeur sur le marché de la cybercriminalité, assorti d'un niveau de protection souvent incomplet, les fragilisent et les constituent en cibles de choix.

En 2023, deux techniques d'intrusion concentrent les plus hauts niveaux de menaces pour les systèmes d'informations des collectivités : le rançongiciel et la compromission de compte des agents.

De quelles cybermalveillances les collectivités sont-elles victimes ?

Le rançongiciel

Logiciel ou virus malveillant, le rançongiciel vient bloquer tout ou partie du système d'information de la collectivité, généralement en chiffrant ses données, c'est-à-dire en les cryptant. Les cyber-assaillants exigent alors une rançon pour fournir une clé de déchiffrement pour rétablir l'accès.

Le vecteur d'attaque initial peut résider dans l'infection d'un premier poste de travail après ouverture d'une pièce jointe ou d'un clic sur un lien reçu en courriel. Une simple navigation sur un site compromis peut également constituer le point d'entrée de l'attaque.

La compromission via les comptes des agents utilisateurs

La faille principale réside dans les comptes de logiciels bureautiques des collaborateurs. L'intrusion est rendue possible par des mots de passe trop faibles ou par le vol d'identifiants via un hameçonnage ou encore par l'utilisation d'accès collectés à l'occasion d'autres cyberattaques.

Info +

Les utilisateurs au premier rang des failles

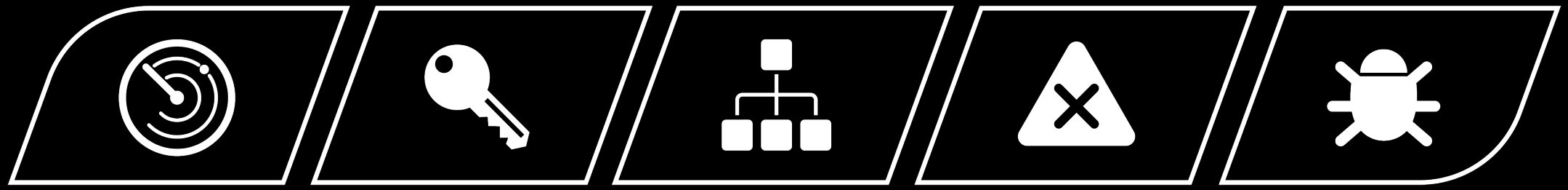
Les attaques dites « zéro clic » sont très rares. Dans plus de 80 % des actions de cybermalveillance observées ces dernières années un utilisateur est impliqué en amont. Une sensibilisation des agents aux menaces et aux bonnes pratiques contribue à limiter les risques.

Info +

Tous les échelons de collectivités sont impactés

Quelles que soient leur taille et leur nature, les collectivités sont victimes d'agissements de cybermalveillance. Ainsi, au cours de l'année 2022 et du premier semestre 2023, on compte parmi les cibles d'attaques aussi bien des métropoles (Lille) que des villes moyennes (Brunoy, Chaville, Frontignan…). Les échelons départementaux (Alpes-Maritimes, Ardèche, Indre-et-Loire, Seine-et-Marne…) et régionaux (Centre-Val-de-Loire, Guadeloupe, Normandie) ont également été impactés sur la même période.

Le mode opérationnel des hackers



Recherche de cibles faciles

- Les adresses IP de sites vulnérables et les identifiants des collaborateurs sont référencés dans des bases de cibles potentielles.

Intrusion dans le système d'information (SI)

- Hameçonnage par e-mail avec lien malveillant.
- Utilisation d'identifiants & mots de passe compromis.
- Téléchargement d'un logiciel malveillant par un collaborateur.

Exploration du SI

- Cartographie des machines, des comptes utilisateurs et des données stratégiques.
- Identification des solutions de sécurité.
- Localisation des sauvegardes.

Prise de contrôle

- Le cyberattaquant renforce son accès en tant qu'utilisateur légitime et se déplace sur le réseau jusqu'à l'atteinte de l'objectif.

Exploitation / attaque

- Chiffrement : cryptage de l'infrastructure.
- Destruction des sauvegardes et exfiltration des données sensibles, dans certains cas.
- Instructions de paiement de rançon.

Info +

La double extorsion

Nouvelle pratique de la cybercriminalité depuis 2021, la double extorsion consiste en un premier temps au chiffrage de l'infrastructure de données de la collectivité, puis à l'exfiltration de ces données sensibles.

Focus expertise

Les petites collectivités sont-elles moins exposées ?

« Toutes les collectivités font aujourd'hui face à des risques élevés car elles détiennent et produisent un grand nombre de données relatives à leurs administrés, très attractives sur le marché de la cybercriminalité.

Les « petites » collectivités sont tout autant exposées que celles de plus grande taille. Or, une commune rurale est soumise aux mêmes règles qu'une métropole. Sa taille ne l'exonère pas de sa responsabilité en matière de protection des données qu'elle collecte auprès de ses habitants ou agents. Et ces données sont en forte croissance, y compris dans ces territoires ruraux, alors même que les personnels sont peu nombreux et les moyens à disposition souvent très limités.

Pour la cybercriminalité, qui est à la fois très créative et très opportuniste, cela peut constituer une cible facile, où le gain sera obtenu sans déployer trop d'efforts. »

Rodrigue Le Bayon,
Responsable du CERT Orange Cyberdefense

Quels sont les risques et les conséquences pour la collectivité ?

Lorsque survient une cyberattaque, la collectivité se trouve confrontée à un maelstrom d'impacts générés par l'indisponibilité de son système d'information, pris en otage. Dans l'attente d'une remédiation qui peut nécessiter plusieurs semaines, les conséquences de l'inaccessibilité des données, des postes de travail ou des réseaux sont immédiates sur l'activité des agents. De même, les services en ligne proposés par la collectivité aux citoyens peuvent être soudainement bloqués.

Des impacts immédiats sur le fonctionnement de la collectivité

Fichiers cryptés, serveurs de la collectivité à l'arrêt… Une cyberattaque, lorsqu'elle est de grande ampleur, peut entraîner au sein des services des perturbations massives.

Pour le cœur d'activité de la collectivité :

- Délivrance de services publics impossible pour les agents en raison du blocage des postes de travail et de l'impossibilité d'accéder aux données des administrés.
- Suspension des outils de messagerie pour contenir la propagation de la menace.
- Mise en place de mesures alternatives de fonctionnement en mode dégradé, chronophages.
- Indisponibilité des services en ligne proposés aux citoyens.
- Perturbation voire indisponibilité des accueils téléphoniques.

Les craintes d'une deuxième vague dans le sillage de l'attaque :

- Risques de divulgation ultérieure de données des agents ou usagers, état-civil, informations bancaires…
- Menaces sur les systèmes de sauvegarde des données, avec risque de destruction par les assaillants.

Des conséquences post-crise

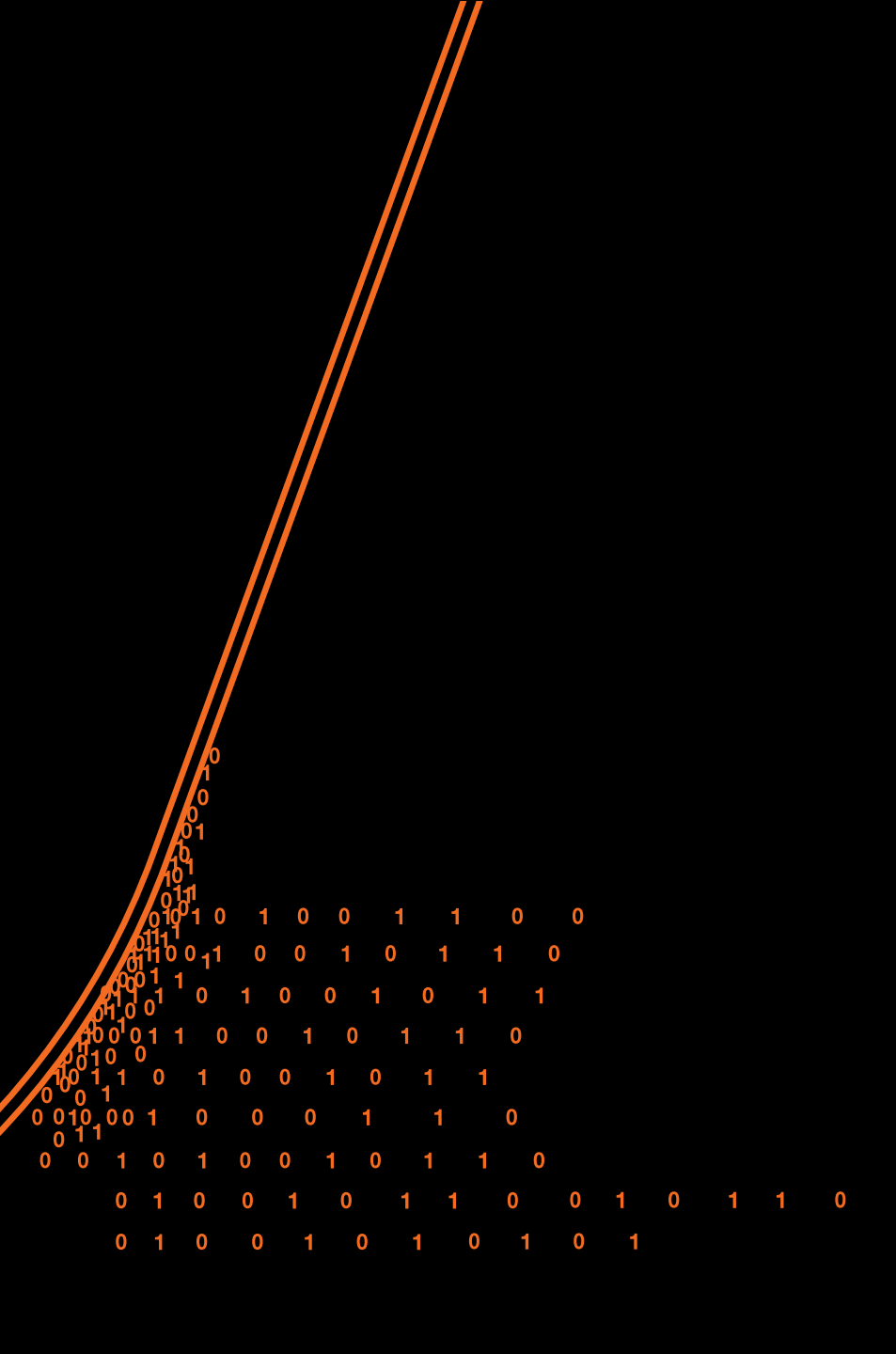
- Impacts d'ordre psychologique pour les agents de la collectivité.
- Atteinte à la réputation et dégradation du lien de confiance aux administrés.
- Pertes financières substantielles.

Quels sont les risques et les conséquences pour la collectivité ?

Un territoire connecté à préserver

Les territoires intelligents offrent des perspectives grandissantes en termes de qualité de vie aussi bien que d'efficacité environnementale. La mise en place de capteurs et de solutions d'Internet des objets pour développer de nouveaux services et optimiser la gestion des infrastructures urbaines a pour corollaire le potentiel d'extension de la surface d'attaque de la collectivité. C'est pourquoi une politique pro-active de cybersécurité a vocation à préserver les acquis et les promesses des smart territoires, dans les usages actuels et à venir, tels que :

- **Gestion connectée des mobilités :** régulation de trafic, feux de signalisation, parking intelligent, bornes de recharges électriques…
- **Applications mobiles** d'information et de services aux citoyens
- **Gestion connectée des infrastructures et services urbains :** collecte des déchets, éclairage public et mobilier urbain, pilotage et hypervision de bâtiments de la collectivité
- **Environnement & sécurité :** surveillance de la qualité de l'air dans des établissements accueillant des publics, surveillance des eaux pour la prévention des risques inondation, vidéo-protection…



Focus réglementation

Sécurité numérique : les obligations et responsabilités des collectivités

Une organisation amenée à traiter des données personnelles doit veiller à garantir trois aspects majeurs : la disponibilité de ces données, leur intégrité et leur confidentialité. Ainsi, une collectivité qui manie des informations personnelles en vue de délivrer un service à ses administrés doit s'assurer de leur accessibilité permanente, de leur non-altération, ainsi que de la protection contre toute intrusion ou interception.

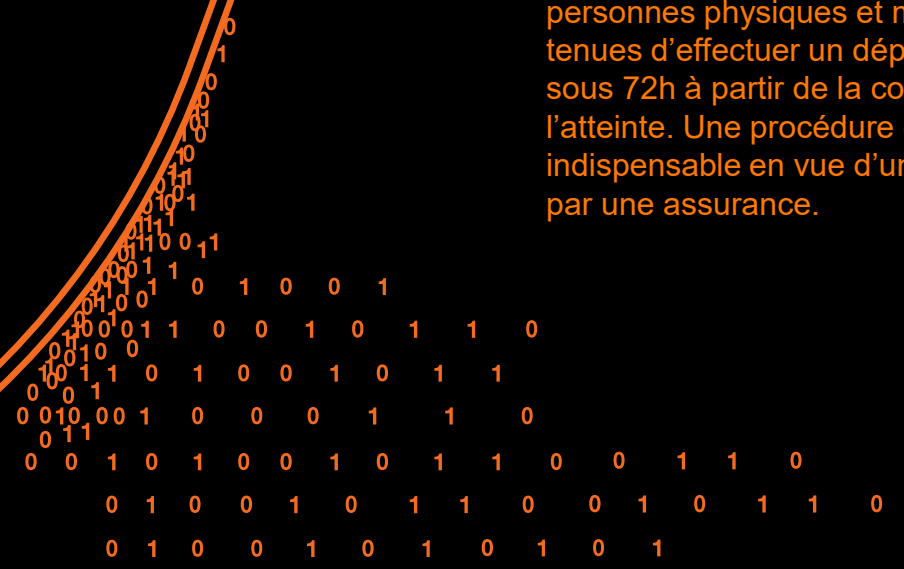
Les autorités gouvernementales, cybermalveillance.gouv et la CNIL rappellent dans un livret co-édité en 2022 les 3 obligations qui s'imposent aux collectivités ainsi qu'à leurs établissements publics :

- la protection des données personnelles,
- la sécurisation des téléservices locaux
- la sécurisation de l'hébergement des données de santé.

En cas de cyberattaque, de dommage ou de méconnaissance de ces obligations, la responsabilité des collectivités ainsi que de leurs agents peut être engagée sur les plans administratif, civil et pénal.

Les obligations RGPD

Selon le règlement général sur la protection des données (RGPD), les collectivités sont tenues, comme tout détenteur de données, d'en signaler toute violation auprès de la CNIL, sous 72 h.



Info +

Directive NIS2 : vers un renforcement des obligations cyber

La transposition en droit français de la directive européenne NIS2, votée en novembre 2022, devrait renforcer les obligations de certaines collectivités locales en matière de cybersécurité, à compter de 2024.

Dépôt de plainte : sous 72h

Depuis avril 2023, en cas de cyberattaque entraînant des pertes ou dommages, les personnes physiques et morales sont tenues d'effectuer un dépôt de plainte, sous 72h à partir de la connaissance de l'atteinte. Une procédure désormais indispensable en vue d'une indemnisation par une assurance.

Comment agir et réagir en cas de cyberattaque ?

Les bons réflexes face à l'urgence

Lorsque survient une cyberattaque, il importe d'adopter des mesures rapides. Les objectifs ? Limiter les différents impacts, assurer au mieux la continuité des services aux administrés et piloter la crise en réduisant au maximum sa durée. Un aperçu des premières dispositions à mettre en œuvre dans des champs essentiels.

Technique

- Stopper la propagation de l'attaque en supprimant les connexions internet et réseaux, en bloquant les accès distants et en isolant les points d'infiltration.
- Renforcer ses capacités d'expertise externe et d'intervention sur les systèmes d'information.

Financier

- Déclarer le sinistre à l'assurance de la collectivité et contacter les services bancaires pour prévenir toute utilisation frauduleuse de données.

Pilotage

- Enclencher le plan de gestion de crise cyber si la collectivité en est dotée.
- Recenser les différents services impactés et coordonner leurs actions.

Administratif

- Procéder à un dépôt de plainte (Police ou Gendarmerie nationale, ou courrier au procureur du TGI).
- Notifier la CNIL dans les 72h en cas de violation de données.

Communication

- Etablir un plan de communication.
- Informer les agents, les administrés et l'ensemble des parties prenantes sur la situation.

Assistance

- Contacter les entités publiques d'appui, qui apportent conseil et orientent vers un prestataire qualifié de réponse à incident (PRIS) :
  - **Le CSIRT** (Computer Security Incident Response Team), centre de réponse de niveau régional aux incidents cyber, en cours de déploiement depuis 2022
  - **L'ANSSI**, Agence nationale de la sécurité des systèmes d'information
  - **Cybermalveillance.gouv**, dispositif national de prévention et d'assistance aux victimes de cybermalveillance

Être accompagné en cas de crise

Contenir l'attaque, enquêter sur les sources de l'intrusion, mettre en œuvre un dispositif de remédiation, optimiser les process de gestion de la crise : Orange Cyberdefense peut mobiliser ses expertises au profit de la collectivité lors d'une crise ou incident cyber.

La réponse aux incidents et l'investigation numérique

- Pour être accompagné de manière réactive par des équipes expertes qui interviennent selon le référentiel d'exigences PRIS (prestataire de réponse à incident de sécurité) défini par l'ANSSI.
- Pour identifier le mode opératoire des assaillants, analyser les programmes malveillants et détecter des intrusions latentes.
- Pour disposer et activer une stratégie de remédiation adaptée : sécurisation des périmètres non encore impactés, éviction de l'attaquant, restauration des données et renforcement du système d'information.
- Pour la mise en évidence et la conservation de preuves en vue d'actions en justice.
- Pour éviter de nouvelles attaques et contribuer à restaurer la confiance des salariés et administrés.

Info +

Pour une capacité de réponse 24/7

Le service de Réponse à incident d'Orange Cyberdefense ouvre l'accès à un support disponible 24h/24, 7j/7, avec une intervention rapide, sur site ou à distance, dans des délais garantis.

Être accompagné en cas de crise

L’accompagnement dans la gestion de crise cyber

- Pour ne pas subir la crise, mais la piloter, en faisant appel à des consultants spécialisés ayant déjà fait face à de multiples situations similaires.
- Pour s’appuyer sur une équipe dédiée, prête à déployer un plan d’action et à actionner un ensemble de procédures et outils.

Info +

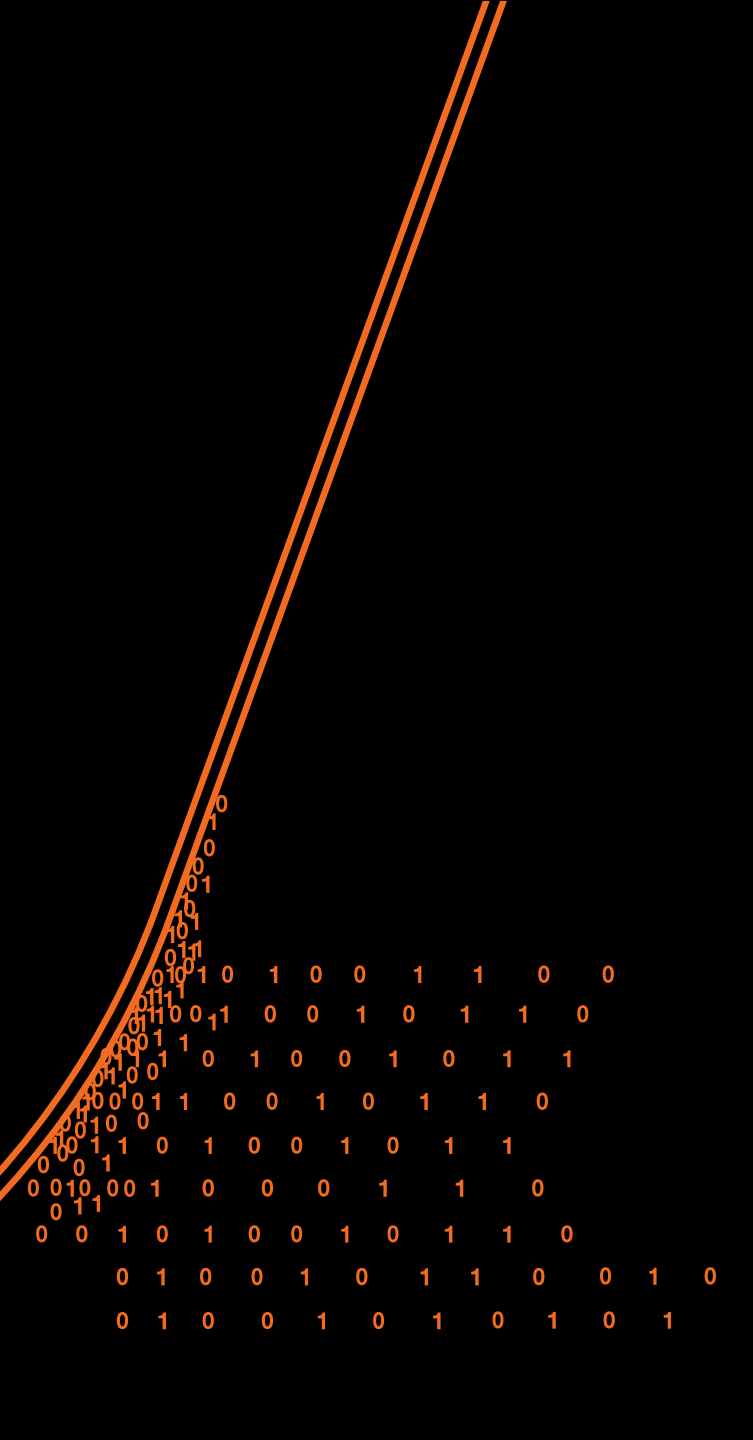
Rançongiciel : faut-il céder ?

Experts et autorités publiques s’accordent sur ce point : il est préférable de ne pas payer de rançon. En effet, céder aux demandes valide le modèle économique des cybercriminels et ne garantit en rien d’éviter la survenue d’une nouvelle attaque.

Info +

Post crise : la cyber résilience

La cyber résilience est la capacité à se préparer et à répondre à de nouveaux évènements dans des conditions en perpétuelle évolution. C’est aussi, en première étape, analyser et comprendre les caractéristiques de l’attaque pour restaurer le système d’information et minimiser les impacts additionnels (fuites de données ultérieures, notamment).



Focus expert

Marc Tolub,
Manager spécialisé en cyber résilience

et Robinson Delaugerre,
Investigations manager au sein d'Orange Cyberdefense

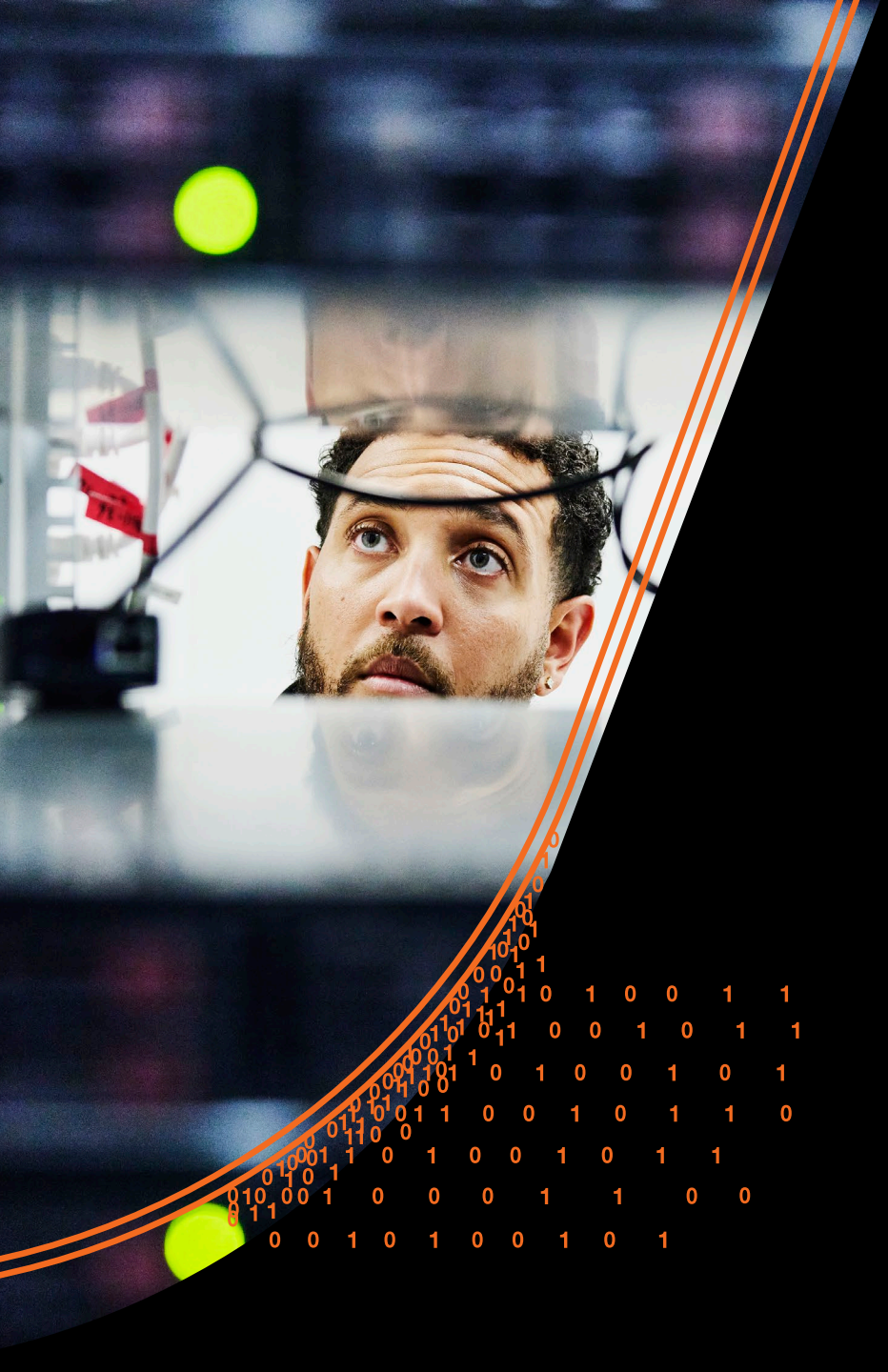
Quelles sont les priorités lors d'une crise cyber ?

« Le premier réflexe doit être de protéger ce qui peut être sauvé, et cela sous-entend de faire des choix difficiles. Lors d'une crise, il faut réagir vite et déterminer ce qui sera protégé en priorité et ce qui sera laissé de côté, ne serait-ce que dans un premier temps. La capacité à gérer au mieux une crise tient souvent dans celle à mobiliser les bonnes personnes en un temps record. »

A contrario, que faut-il éviter ?

« Moins une organisation est préparée à une crise cyber, plus les impacts seront graves et difficiles pour elle. Cela étant, même pour les entités préparées, l'un des moins bons réflexes que nous avons pu observer est celui de décisions prises à la hâte, avant même de disposer de tous les éléments. Lors d'une crise, on court après le temps, mais il ne faut pas confondre vitesse et précipitation : les mauvaises décisions augmentent les impacts négatifs d'une crise de manière considérable.

Enfin, les crises cyber ont la particularité d'être transverses. Dès le début de la crise, il est nécessaire de mobiliser l'ensemble des acteurs, qu'ils soient techniques ou fonctionnels. »



Focus collectivité

Chalon-sur-Saône : limiter la propagation et ses impacts

Un dimanche de février 2021, au petit matin, la commune de Chalon-sur-Saône détecte une activité anormale sur le parc informatique de sa police municipale. Quelques minutes plus tard, le diagnostic d'une cyberattaque de grande ampleur par cryptovirus est confirmé.
La collectivité prend immédiatement les premières mesures conservatoires, en mettant à l'arrêt les sauvegardes, les accès internet ainsi que les serveurs.

Dès le lendemain, Orange Cyberdefense est missionné après mise en relation par l'ANSSI pour accompagner la Ville et le Grand Chalon dans un plan d'action associant gestion de crise, investigation numérique, remédiation et reconstruction du système d'information.

« Les équipes d'Orange Cyberdefense étaient intervenues une semaine auparavant sur le même cryptovirus à l'hôpital de Villefranche-sur-Saône. Parmi les mesures techniques, nous avons déployé sur nos 200 serveurs et 1400 postes de travail leur service anti-malware supervisé en temps réel. Dans le même temps pour garantir la continuité des services, nous avons équipé en urgence des salles dédiées de co-working.

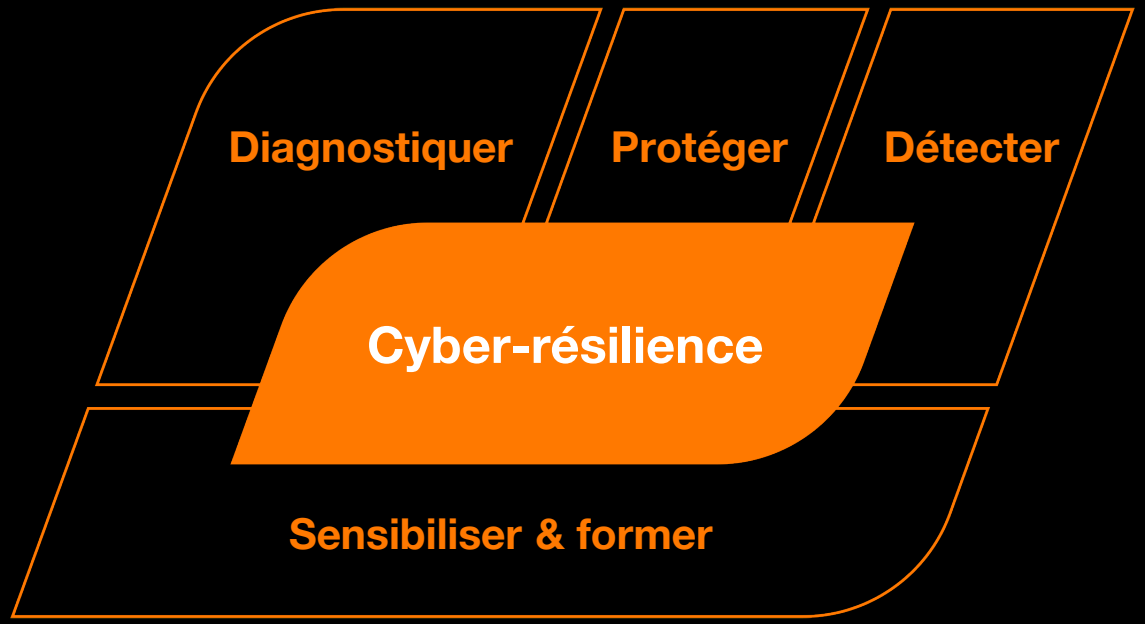
Le rétablissement a été mené de manière progressive, par étapes : installation d'une nouvelle infrastructure, restauration des sauvegardes puis remise en ligne des serveurs et applications critiques. C'est au 30 juin que l'accès internet a pu être réouvert. La phase de remédiation aura duré environ 3 mois. Au 31 décembre, 90 % du SI était reconstruit.

Nous en avons tiré des enseignements : la menace ne peut être éradiquée, l'objectif est d'en limiter la propagation et les impacts, en définissant un plan d'action préventif adapté. Il est notamment essentiel de sensibiliser et former les collaborateurs, dresser un état des lieux, renforcer la sécurité des équipements, cloisonner le SI et définir des règles de gouvernance. »

Frédéric Iacovella
Directeur général des services
Ville de Chalon-sur-Saône et Grand Chalon

Comment anticiper pour prémunir la collectivité des cybermenaces ?

Les évènements traités par les centres de réponse à incidents d'Orange le montrent : plus les entités sont préparées et ont anticipé un dispositif de gestion de crise, mieux elles font face à une cyberattaque. Les collectivités peuvent gagner à mettre en place des plans d'actions pour une cyberprotection adaptée à leurs besoins, à leur taille et à leur degré de maturité, et développer ainsi leur cyber résilience.



Info +

France Relance :
Orange aux côtés des collectivités

Dans le cadre du plan Cyber France Relance visant à renforcer le niveau de sécurité de l'administration française, Orange a accompagné plus de 200 collectivités (communes, intercommunalités, Conseils départementaux et Régions).

Diagnostiquer

La mesure de l'exposition aux risques et l'identification des menaces qui peuvent peser sur la collectivité constituent une étape essentielle : un prérequis pour organiser sa cyber-résilience.

Le diagnostic de cybersécurité

- Pour obtenir un état des lieux du niveau de sécurité du système d'information de la collectivité et éprouver sa robustesse, au moyen d'un audit organisationnel qui s'appuie sur le référentiel de l'ANSSI.
- Pour activer des tests techniques qui mettent à jour les vulnérabilités.
- Pour disposer de recommandations organisationnelles et techniques, formalisées en un plan d'actions et une feuille de route opérationnelle.

Des tests d'intrusion en conditions réelles

- Pour contrôler le niveau d'exposition aux menaces en mettant à l'épreuve le système d'information de la collectivité pour détecter ses failles d'infrastructure.
- Pour disposer de préconisations d'actions correctives.

Des services de veille et de gestion des vulnérabilités

- Pour maintenir le niveau de sécurité de la collectivité au moyen d'une approche par les risques.
- Pour disposer d'alertes sur les nouvelles vulnérabilités en temps réel et protéger les activités les plus critiques.
- Pour déterminer avec précision les failles dans le but de prioriser les actions correctives et ainsi réduire la surface d'attaque potentielle.

Info +

Des Pentests menés par des hackers éthiques

Les services de pentests, ou tests de pénétration, ont pour but d'éprouver en conditions réelles la capacité d'assaillants à entrer dans le système d'information d'une collectivité. Des hackers éthiques testent les points d'entrée les plus exposés : sites Internet, réseaux, applicatifs, e-mails ou encore téléphones et badges d'accès. Outre la vulnérabilité des infrastructures, l'approche évalue aussi la perméabilité aux attaques liée au facteur humain. Des simulations de phishing, avec l'envoi d'e-mails compromis aux personnels de la collectivité, permettent notamment d'évaluer les méthodes de signalement d'un courriel suspect.

Protéger

Face à une cybercriminalité opportuniste, touchant en premier lieu les cibles qui présentent les moindres protections, il est essentiel de mettre en place des boucliers efficaces pour préserver le système d'information de la collectivité.

Une solution de protection clé en main

- Pour mettre en place un dispositif complet contre les menaces : contrôle des flux internet, protection du trafic de messagerie, ainsi que des serveurs et postes de travail, détection d'intrusions et d'applications vulnérables, tunnels chiffrés pour raccorder des sites distants et collaborateurs nomades, protections anti-malware, anti-spam et antiphishing…
- Pour disposer d'une solution sécurisée, intégrée dans le cloud d'Orange, avec le support d'une plateforme d'experts.

L'externalisation des sauvegardes et la reprise d'activité

- Pour rendre les sauvegardes inaccessibles aux attaques, en veillant à les cloisonner avec un hébergement dans un cloud de confiance.
- Pour restaurer les capacités de traitement après une cyberattaque.
- Pour disposer d'une solution de secours managée : maintien en condition opérationnelle, tests réguliers, garanties de services…

Une protection priorisant les messageries

- Pour protéger les boîtes mails, sans aucune infrastructure à installer, en générant un reporting complet.
- Pour préserver son activité en évitant les erreurs humaines qui peuvent bloquer le système d'information de la collectivité (hameçonnage).

Info +

L'e-mail, base de 90 % des attaques

La messagerie électronique constitue une cible privilégiée par les pirates informatiques pour répandre des programmes logiciels malveillants. Pas moins de 90 % de ces malwares transitent en effet via les e-mails.

Source : Vade Secure

Protéger

La gestion des identités et des accès

- Pour gérer les droits d'accès au système d'information, tout au long du cycle de vie d'un utilisateur au sein de la collectivité (embauche, mobilité interne, évolution hiérarchique, départ…).
- Pour mettre en place une stratégie de gouvernance et d'administration des identités (IGA) qui renforce la sécurité numérique, tout en répondant aux exigences règlementaires françaises et internationales.

La sécurité des clés USB

- Pour détecter et supprimer les logiciels malveillants sur les supports amovibles (clé USB, disque dur externe…), avec un dispositif pouvant être mis en place sur une borne disponible dans les espaces partagés par les agents.

Info +

La clé USB, toujours un vecteur de menace

Alors que 44 % des clés USB contiendraient au moins un dossier comportant des risques (source Honeywell), plus des deux tiers des salariés ne prennent aucune protection avant de les insérer sur leur PC (source Ponemon). Ces périphériques souvent considérés comme anodins figurent au deuxième rang des cybermenaces les plus dangereuses (classement BSI-CS).

La protection des terminaux mobiles

- Pour équiper ses agents nomades d'une solution avancée de détection préventive des menaces.
- Pour disposer de l'état sanitaire des données de la flotte de terminaux mobiles via un portail de reporting.

Surveiller et détecter

Les offensives des cybercriminels se renouvellent et se perfectionnent constamment, dans leurs techniques et modes opératoires. Pour déjouer les attaques, préserver le patrimoine informationnel de la collectivité et garantir sa continuité d'action au service des citoyens, il importe de se prémunir au moyen d'outils de surveillance et de détection adaptés.

Un portail d'administration des usages internet

- Pour disposer d'une plateforme qui contrôle l'ensemble des usages et des flux internet : surveillance du trafic entrant et sortant, connexions à distance, filtrage des sites web et applications, prévention d'intrusions, protection anti-malware, gestion des droits différenciés selon les collaborateurs…
- Pour permettre aux responsables du système d'information de mettre en œuvre une politique de sécurité et de l'administrer, en mode local ou sur un cloud.

Surveiller et détecter

Une solution de détection des incidents de sécurité (SOC)

- Pour protéger les postes de travail ainsi que les serveurs de la collectivité, au moyen d'une plateforme de supervision de la sécurité du système d'information, couplée à l'expertise d'analystes en surveillance continue.
- Pour réduire le temps de réaction, détecter les indices de compromission et contenir les menaces au plus tôt.
- Pour bloquer les attaques, avec une suppression automatique des fichiers infectés, tout en conservant une capacité d'intervention sur son parc informatique, grâce à un portail personnalisé permettant de confiner les postes compromis.
- Pour se reposer sur une solution alliant surveillance, confinement, investigation et remédiation, avec un contrôle permanent intégrant des alertes pro-actives et qualifiées par des experts en Threat Intelligence.

Info +

Une plateforme SOC, combien ça coûte ?

Contrairement aux idées reçues, recourir à un SOC pour protéger son système d'information contre les cyberattaques peut constituer un investissement très abordable. Ainsi, les offres Micro-SOC d'Orange Cyberdefense débutent à partir de 2,50 € par mois et par poste de travail.

Info +

L'IA et le renseignement au service de la cybersécurité des territoires

Orange Cyberdefense traite quotidiennement 60 milliards d'évènements par jour.
Pour le traitement de ce volume croissant de données généré par les menaces cybercriminelles, les experts de l'entité s'appuient toujours plus sur les nouvelles technologies de l'intelligence artificielle, associées au cyber-renseignement, grâce à un datalake (lac de données) de plus de 400 sources.

Sensibiliser et former

En parallèle aux 3 étapes essentielles de diagnostic, protection et détection des cybermalveillances, la sensibilisation et la formation des équipes internes demeurent nécessaires, au long cours. Non seulement du fait de l'évolution constante des menaces, mais aussi parce que les effectifs et l'organisation d'une collectivité sont soumis à des mutations continues.

La sensibilisation et la communication sur la cybersécurité

- Pour faire prendre conscience des risques afin de limiter les failles humaines, principale source de compromission, essentiellement par méconnaissance des menaces.
- Pour communiquer et diffuser de bonnes pratiques au sein des services de la collectivité, au moyen d'une palette de supports tels que guides, flyers, posters, contenus vidéo et motion design…
- Pour sensibiliser les agents via des sessions thématiques qui intègrent une personnalisation des règles de sécurité numérique, associées à des modules de contrôles des acquis (quiz, campagnes-tests de phishing…).

La sensibilisation par le jeu

- Pour marquer les esprits, en associant les techniques d'e-learning à l'approche par le jeu, ou comment acquérir les bons réflexes d'hygiène numérique dans le cadre d'un apprentissage collaboratif et ludique.
- Pour compléter les sessions de sensibilisation de formats plus classiques.

Sensibiliser et former

Des formations expertes

- Pour permettre une montée en compétence des professionnels de la sécurité du système d'information (SI) de la collectivité, au moyen de formations techniques, organisationnelles et certifiantes.
- Pour bénéficier de contenus de formation élaborés par des experts en cybersécurité, connectés aux réalités métiers : des cas concrets agrémentés de retours d'expérience.

Info +

Se former aux enjeux de la cybersécurité des collectivités

L'offre de formations Cyberdefense Education s'attache à suivre les évolutions rapides des risques et menaces qui pèsent sur les organisations. Les thématiques couvrent les grands enjeux de la cybersécurité auxquels sont confrontés les collectivités, tels que la conformité aux règlementations et le respect des obligations légales, la connaissance des nouvelles menaces et savoir anticiper les attaques ou encore la sécurisation du système d'information.

Focus collectivité

Saint-Leu : « un vrai déclic » pour la cybersécurité

Consciente de la nécessité de protéger ses données, la mairie réunionnaise de Saint-Leu (31 000 habitants, 600 agents, 250 postes informatiques) a mis à profit le plan France Relance pour structurer sa politique de cybersécurité.

Dans ce cadre, les experts d'Orange Cyberdefense ont réalisé un audit complet de la sécurité du système d'information de la collectivité. Cet état des lieux organisationnel et technique a révélé dans un premier temps plusieurs vulnérabilités. Une feuille de route a ensuite été établie, comprenant des axes d'amélioration : poursuivre la sécurisation du poste de travail, maitriser l'accès aux ressources informatiques en production et renforcer la protection des échanges internet.

Un accompagnement qui intégrait également des actions de sensibilisation du personnel manipulant les données les plus sensibles, ainsi que quatre jours de formation des membres du service informatique aux bonnes pratiques de cybersécurité.

« Le nombre d'attaques informatiques dans le secteur public est exponentiel. Nous avons souhaité nous inscrire dans une logique de prévention pour protéger au mieux nos données. C'est un enjeu de réputation, mais aussi de confiance des administrés.

Pour nous accompagner, nous avons choisi Orange Business avec qui nous collaborions déjà sur d'autres prestations. Nous travaillons avec les experts locaux d'Orange Cyberdefense Océan Indien, tout en ayant l'assurance de pouvoir nous appuyer sur l'ensemble du Groupe. Le calendrier a bien été respecté. Le cadrage, la méthodologie et les livrables suivaient au plus près le référentiel défini par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Ce travail a constitué un vrai déclic, y compris pour les décideurs. Tout le monde avance maintenant dans le même sens pour mettre en œuvre notre feuille de route, avec davantage de budgets alloués à la sécurité numérique ».

Jean-David Irsapoullé,
DSI de la Mairie de Saint-Leu

Orange Cyberdefense

Construire une société numérique plus sûre, au cœur des territoires

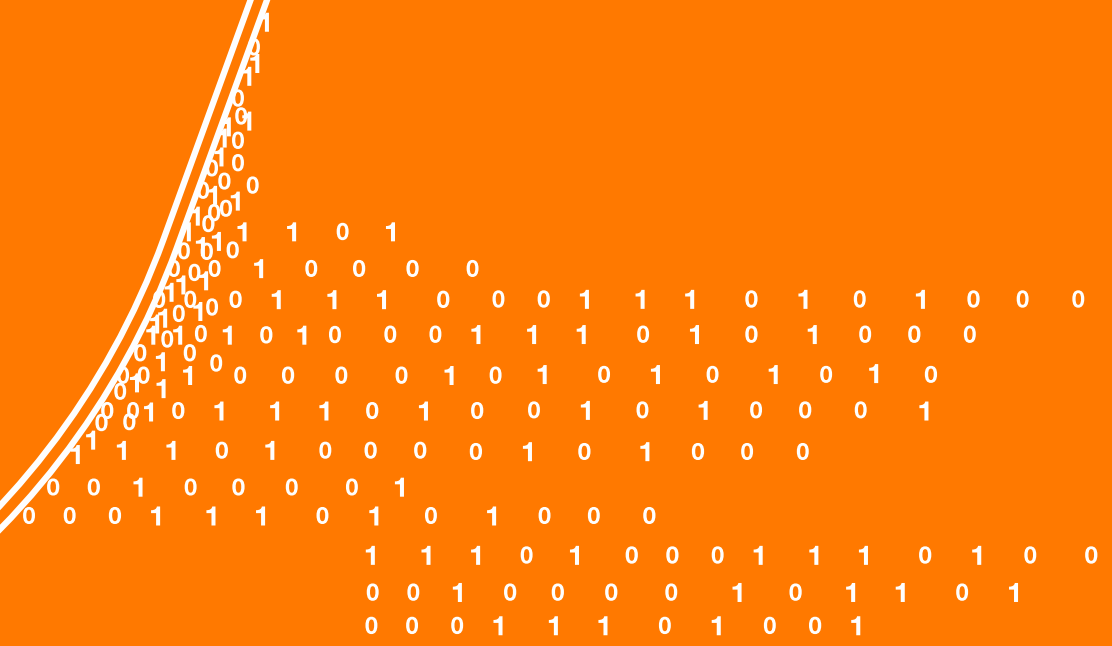
Orange est présent partout en France pour accompagner les collectivités dans leur cybersécurité, avec des réponses adaptées aux différentes échelles territoriales.

Orange Cyberdefense, l'entité stratégique du Groupe Orange dédiée à la sécurité numérique

La sécurité est devenue un grand métier d'Orange et un élément important de sa stratégie, pour construire une société numérique plus sûre. Leader européen de prestations de services en cybersécurité, Orange Cyberdefense accompagne la transformation numérique de ses clients : entreprises de toutes tailles, organismes critiques, administrations et collectivités locales.

Ses équipes, composées de plus de 3000 experts, protègent aujourd'hui plus de 8500 entités en France et dans le monde afin d'assurer le meilleur niveau de protection de leurs données, de leurs équipements et des services qu'ils offrent à leurs clients ou à leurs administrés.

- **Plus de 300 collectivités accompagnées par Orange Cyberdefense**
- **60 milliards d'évènements collectés et analysés chaque jour**
- **50 jours d'avance dans la détection des menaces**
- **Une surveillance des infrastructures 24/7/365**



Liens et contacts utiles

Pour les offres proposées aux collectivités

orangecyberdefense.com/fr/services

orange-business.com/fr/secteurs-et-metiers/smart-cities-et-territoires

Pour bénéficier d'une vue d'ensemble sur la cybersécurité avec le rapport Security Navigator 2023

orangecyberdefense.com/fr/insights/security-navigator

Pour sécuriser les usages numériques des collectivités territoriales avec Orange Cyberdefense

orangecyberdefense.com

Pour contacter votre délégation régionale Orange

collectivites.orange.com/fr/contacts-par-regions/