TRANSITION NUMÉRIQUE

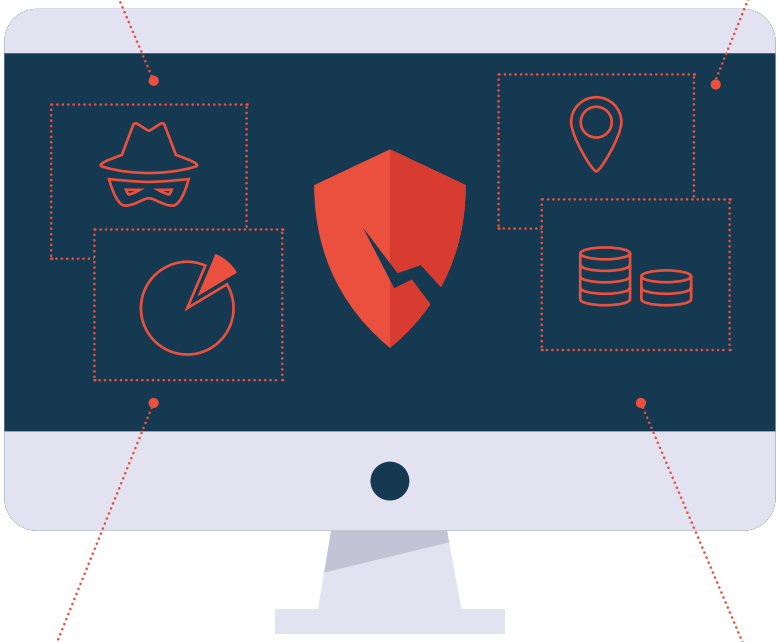
CYBERSÉCURITÉ
COMMENT LA GARANTIR AU SEIN DE SA COLLECTIVITÉ

SIPPEREC
ÉNERGIES ET NUMÉRIQUE

La crise sanitaire a accéléré la transformation numérique des collectivités. En parallèle, les attaques informatiques se sont multipliées à la vitesse d'une pandémie. Les pirates exploitent les failles des ordinateurs et des réseaux mal protégés. Face à ce fléau, le SIPPEREC vous propose des solutions pour garantir la sécurité de vos systèmes informatiques.

23 %
des attaques par rançongiciel ont visé des collectivités en 2022.

43
collectivités d'Île-de-France officiellement touchées depuis 2020.



L'investissement annuel nécessaire à la cybersécurité est évalué entre
5 et 10 %
du budget informatique.

Le coût d'une cyberattaque se chiffre en
centaines de milliers voire en millions d'euros.

DES ACTIONS PRIORITAIRES À FAIRE

1

La conduite du changement et la sensibilisation des agents de la collectivité qui, par leur comportement, peuvent multiplier ou réduire les risques.

2

La vision claire des systèmes d'information employés et leur pertinence en termes d'activité et de services rendus avec un inventaire patrimonial des systèmes d'information, des installations matérielles et des applications, sous la forme d'une cartographie, une évaluation du risque numérique généré par chacun d'entre eux et, enfin, un plan d'action de réduction des risques.

3

L'analyse des clauses contractuelles des marchés de prestations informatiques intégrant ou pas le risque numérique.

4

L'élaboration d'un plan de crise numérique pour savoir quoi faire en cas de cyberattaque, afin d'assurer la continuité de service et la reprise d'activité.

BON À SAVOIR

La mutualisation des ressources dédiées à la cybersécurité au sein de l'intercommunalité constitue un moyen d'optimisation des coûts et de garantie de sécurisation des systèmes d'information.

Source : www.amf.asso.fr

DES OBLIGATIONS AU NIVEAU DES COLLECTIVITÉS

Les collectivités territoriales sont soumises à un cadre réglementaire qui vise à renforcer la confiance des usagers dans l'utilisation des services en ligne et à protéger les données à caractère personnel.

LE RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ (RGS)

est le cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.

Source : www.ssi.gouv.fr

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

est entré en application le 25 mai 2018. Il harmonis les règles et les pratiques européennes, applicables en matière de protection des données à caractère personnel. Entreprises de toutes tailles, administrations et collectivités qui traitent des données à caractère personnel, sont concernées.

Source : www.ssi.gouv.fr

LE RÈGLEMENT « EIDAS » N° 910/2014 DU 23 JUILLET 2014

établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

Source : www.ssi.gouv.fr

DES RESSOURCES
DANS LE PLAN DE RELANCE

Dans le cadre du volet cybersécurité du plan France Relance, le gouvernement attribue 136 millions d'euros (30 millions d'euros supplémentaires en 2023) à l'État, aux collectivités territoriales, aux organismes au service des citoyens, pour renforcer et accélérer leur niveau de cybersécurité. Le pilotage en est confié à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui peut accompagner les actions des collectivités territoriales de toutes tailles, selon leur niveau de maturité dans la sécurisation de leur système d'information.

Source : www.ssi.gouv.fr/agence/cybersecurite

LES PRINCIPALES MENACES

L'HAMEÇONNAGE
(phishing en anglais)

C'est une technique frauduleuse destinée à **leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires,** en se faisant passer pour un tiers de confiance pour en faire un usage frauduleux. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administration, etc.

Sources : www.cybermalveillance.gouv.fr/cybermenaces

LES RANÇONGICIELS

(ransomwares en anglais)

Ils bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et réclament à la victime le paiement d'une rançon en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou, encore, suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

LA DÉFIGURATION DE SITE WEB

C'est l'**altération par un pirate de l'apparence d'un site Internet**, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l'objet initial du site. La défiguration est le signe visible qu'un site Internet a été attaqué et que l'attaquant en a obtenu les droits lui permettant d'en modifier le contenu. Par ailleurs, en étant visible publiquement, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc accéder potentiellement à des données sensibles, ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site Internet.

L'ATTAQUE EN DÉNI DE SERVICE

(DDoS pour Distributed Denial of Service en anglais)

Elle vise à **rendre inaccessible un serveur** par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles.

Des solutions disponibles via SIPP'n'CO

Le SIPPEREC propose un large panel de solutions de sécurisation des systèmes d'information (SI) :

Un marché d'assistance à maîtrise d'ouvrage dédié à la cybersécurité (bouquet 4) pour :

- la gouvernance de la sécurité des SI : assistance au Responsable de la sécurité des SI (RSSI), rédaction de la Politique de sécurité des systèmes d'information (PSSI), diagnostic cybersécurité… ;
- l'expertise technique en cybersécurité (architecture système et réseau, gestion des incidents, Plan de reprise d'activité, Plan de continuité d'activité…) ;
- l'audit technique : analyse de risque, audit d'intrusion, de configuration, de code, de sécurité Office 365…

Un marché d'assistance à maîtrise d'ouvrage dédié aux infrastructures numériques (bouquet 4) pour :

- sécuriser les salles serveurs, les installations téléphoniques (IPBX), les sauvegardes ;
- la mise en œuvre d'un Plan de reprise d'activité (PRA), d'un Plan de continuité d'activité (PCA) ;
- déployer une solution collaborative externalisée et sécurisée (messagerie électronique, visioconférence, partage de documents…).

Un marché dédié à la mise en œuvre des solutions de sécurisation (bouquet 4) comprenant :

- les services, prestations, équipements et logiciels pour garantir la sécurité des SI : pare-feu, proxy, antivirus, détection de vulnérabilité, détection et prévention d'intrusion, sécurisation des accès et des données, prestations de mise en œuvre de la sécurité fonctionnelle…

Un ensemble de marchés de maîtrise d'œuvre et d'assistance à maîtrise d'ouvrage permettant d'exploiter en toute sécurité :

- les services de téléphonie fixe et mobile (bouquet 3) ;
- l'interconnexion VPN, les accès Internet, les infrastructures numériques du bouquet 4 (solutions collaboratives dans le cloud, infrastructures systèmes, réseaux, télécommunications, postes de travail) ;
- les solutions intelligentes de sécurité et sûreté dans les bâtiments et dans l'espace public (bouquet 5) ;
- les équipements numériques éducatifs (bouquet 6) ;
- les solutions de Gestion de la relation avec les usagers (bouquet 6).

Un marché dédié à la mise en œuvre du Règlement général sur la protection des données (RGPD) qui constitue l'occasion idéale de diffuser une culture de la cybersécurité au sein des collectivités. (bouquet 6).

L'offre de services d'achat mutualisé du SIPPEREC apporte également des solutions concrètes et adaptées pour faciliter **le déploiement du télétravail en toute sécurité.**

Offre de marchés à retrouver dans les bouquets 3 à 6 de SIPP'n'CO.

Plusieurs sites Internet ressources pour aller plus loin :

Cybermalveillance.gouv.fr

Banque des Territoires

Association des Maires de France / ANSSI :

Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) :

- Attaques par rançongiciels, tous concernés – comment les anticiper et réagir en cas d'incident ?
- Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation
- Guide d'hygiène informatique

Commission Informatique et Libertés (CNIL)

VOTRE CONTACT AU SIPPEREC

SERVICE RELATIONS ADÉRENTS

adherents@sipperec.fr

Syndicat Intercommunal de la Périphérie de Paris pour les Énergies et les Réseaux de Communication (SIPPEREC)
Tour Lyon Bercy - 173 / 175 rue de Bercy - CS 10205 - 75588 Paris cedex 12
Tél. : 01 44 74 32 00 | **E-mail :** communication@sipperec.fr

Directeur de la publication : Jacques J.-P. MARTIN
Rédaction : Direction de la communication du SIPPEREC
Conception/réalisation : Agence 4août
Impression : MERICO - Mai 2021

Suivez-nous sur @sipperec_idf
www.sipperec.fr

FSC RECYCLÉ FSC® C016838