

Rapport :

Panoramas des cyber attaques les plus significatifs de 2022.



Introduction

En 2022, les cyberattaques ont continué de faire les gros titres de l'actualité, touchant de nombreux secteurs d'activité. La santé, la finance, les transports, l'énergie et les services publics ont été particulièrement touchés. Le phishing, les rançongiciels et les attaques DDoS sont devenus monnaie courante. Si ces termes ne vous sont pas familiers, n'hésitez pas à jeter un coup d'œil au premier rapport :

Aperçu des cyber menaces les plus répandues sur l'année 2022.

Dans ce contexte, il est crucial pour les entreprises et les organisations de prendre des mesures pour protéger leurs systèmes informatiques et leurs données sensibles contre les cyberattaques.

Dans ce rapport, nous examinons les cyberattaques les plus significatifs de 2022.

Le but de ce travail est de comprendre les dernières tendances en matière de cyberattaques et de proposer une vue global sur les activités cyber de l'année passée.

Sommaire

Principaux Hôpitaux Français.....	3
Grands comptes privés touchés.....	6
Les régions attaquées	8
Les départements touchés	10
Les communes de plus de 5 000 habitants ciblés	12
Sources.....	17

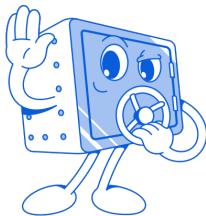
Principaux Hôpitaux Français

Clinique Léonard de Vinci de Chambray-les-Tours

La Clinique Léonard-de-Vinci de Chambray-les-Tours a été victime d'une cyberattaque le 7 janvier 2022, celle-ci a été commise par un groupe de hackers expérimentés utilisant une technique de **rançongiciel pour verrouiller les systèmes informatiques de l'établissement**.

Lors de cette attaque, les malfaiteurs ont **crypté les fichiers de la clinique, empêchant ainsi l'accès aux dossiers des patients**. Cette indisponibilité s'est poursuivie plusieurs jours, causant l'annulation de la quasi-totalité des opérations prévues. Les laboratoires de test médicaux, la médecine nucléaire et la pédiatrie ont toutefois pu continuer à fonctionner car les données de ces services étaient **stockées sur un autre serveur**.

Ces pirates informatiques ont également demandé **une rançon de 500 000 € pour débloquer le système informatique de la clinique**.



Il est important de souligner que payer la rançon ne garantit pas que les fichiers seront débloqués ou récupérés. Il est donc important de se protéger contre les attaques de rançongiciels en utilisant des logiciels de sécurité, en effectuant régulièrement des sauvegardes de données et en étant vigilant face aux courriels de phishing et aux téléchargements malveillants.

Cité sanitaire de Saint-Nazaire

La société **AKLIA**, prestataire de la cité sanitaire de Saint-Nazaire a été victime d'une cyberattaque le 12 janvier 2022, les services de télévision, téléphonie, et le Wi-Fi de l'établissement ont **cessé de fonctionner pendant plusieurs jours**. Peu d'informations ont été communiquées sur cette attaque. Mais en raison de cet évènement, le personnel hospitalier a rencontré des difficultés pour être contactées. Les équipes de la Cité sanitaire et de AKLIA ont alors activement travaillé pour essayer résoudre cette situation et retrouver un fonctionnement normal le plus rapidement.

À noter que les soins des patients n'ont pas été impactés par cette cyberattaque.

L'hôpital de Saint-Dizier et de Vitry-le-François

L'hôpital de Saint-Dizier et de Vitry-le-François ont été victimes d'une cyberattaque le 19 avril 2022, celle-ci a été commise par un groupe de **pirates informatiques utilisant un logiciel de rançongiciel pour verrouiller les systèmes informatiques de l'établissement**.

Les pirates ont réussi à infiltrer le réseau internet du groupement hospitalier de territoires Grand-Est, qui gère huit hôpitaux, et ont **dérobé des données sensibles**, comme des factures, des coordonnées et des numéros de sécurité sociale. Les connexions internet avec l'extérieur ont été immédiatement suspendues pour limiter la propagation de l'attaque et protéger les données de l'hôpital.

Ils ont également menacé l'établissement de **verser une rançon de 1,3 million de dollars** pour débloquer les systèmes informatiques. Mais **certaines copies de fichiers volés avait déjà été retrouvée sur le darknet**.

Principaux Hôpitaux Français

Centre Hospitalier de Mâcon

Le Centre hospitalier de Mâcon a été touché le 27 mai 2022. Pour stopper l'attaque, la direction des systèmes d'information a **isolé complètement l'hôpital du réseau**. Cela s'est traduit par l'arrêt pendant une dizaine de jours de l'ensemble des flux internet et de la messagerie.

Pour s'assurer que l'attaque ne se reproduit pas, **une analyse complète a été effectuée sur l'ensemble du système avec l'aide et l'expertise** des instances nationales telles que l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information) et le **CERT Santé** (Centre d'Expertise et de Réponse aux Attaques des systèmes d'Information de santé).

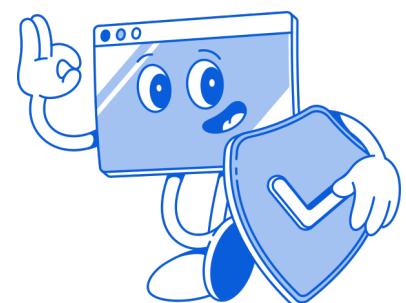
Centre Hospitalier de Corbeil-Essonnes

Le Centre hospitalier de Corbeil-Essonnes a été victime d'une cyberattaque de grande ampleur le samedi 20 août 2022. **Cette attaque a été revendiquée par le groupe Lockbit**, dont certains membres sont soupçonnés d'opérer depuis la Russie. Les pirates ont utilisé un **logiciel de rançongiciel pour bloquer les systèmes informatiques de l'établissement**.

Lors de cette attaque, les pirates ont dérobé des données sensibles, notamment des données de santé des usagers, des membres du personnel et des partenaires de l'hôpital. Ils ont également **exigé une rançon de 10 millions de dollars** pour libérer les systèmes informatiques de l'hôpital. Selon zataz.com, les pirates ont ensuite réclamé à l'hôpital "**2 millions de dollars (1 million pour détruire les données volées et un million pour rendre l'accès aux informations via leur logiciel dédié)**".

Ils avaient fixé un ultimatum au 23 septembre pour que l'hôpital paye la rançon. Ils ont tout de même **commencé à diffuser les données dérobées**. Sur leur site internet, une archive compressée de plus de 11 giga-octets a été mise en ligne et est proposée au téléchargement. **L'activité de l'hôpital est revenue à la normale à la mi-octobre**, grâce aux efforts de l'équipe de l'hôpital et de l'**ANSSI** (Agence Nationale de la sécurité des systèmes d'information) pour contenir l'attaque et protéger les données.

Il est également important de rappeler que la protection de la vie privée et des données sensibles des patients, des employés et des partenaires de l'hôpital est une priorité absolue et toutes les mesures appropriées doivent être prises pour éviter une récidive de ce genre d'attaques.



Hôpital de Cahors

Le 12 septembre, l'Hôpital de Cahors a été victime d'une cyberattaque. L'Agence numérique en santé (ANS) a détecté une intrusion dans le système informatique de l'établissement, visant principalement la messagerie interne. **L'hôpital a immédiatement été alerté de cette intrusion**.

Heureusement, **les données informatisées des patients sont indemnes car elles sont hébergées chez un autre prestataire**.

Principaux Hôpitaux Français

Centre Hospitalier de Versailles

L'Hôpital André-Mignot de Versailles a été victime d'une cyberattaque le 3 décembre 2022 **par le groupe connu sous le nom de LockBit 3.0, utilisant un logiciel de rançongiciel (ransomware)**.

Heureusement, l'attaque a été détectée tôt, ce qui a permis de mettre en place rapidement des mesures de protection pour limiter les dégâts. Malgré cela, plusieurs patients ont dû être transférés vers d'autres établissements pour poursuivre leur traitement. Heureusement, le SAMU n'a pas été impacté par cette attaque et les nouveaux patients ont pu être pris en charge dans les plus brefs délais.

Centre Hospitalier d'Argenteuil

Le Centre hospitalier d'Argenteuil a failli être victime d'une cyberattaque début décembre (mercredi 7 décembre 2022). **Une double tentative d'intrusion** dans son système informatique a été repérée par les équipes informatiques de l'hôpital. Des mesures ont rapidement été prises pour arrêter l'attaque et protéger les données de l'établissement.

Heureusement, **l'activité hospitalière n'a pas été perturbée** et l'ensemble des services de l'hôpital sont restés opérationnels. La direction de la sécurité informatique du Centre hospitalier d'Argenteuil a fait savoir qu'elle était pleinement mobilisée pour protéger les intérêts des patients, des partenaires et des employés de l'hôpital.

Le fait que le Centre hospitalier d'Argenteuil **travaille en étroite collaboration avec les experts de l'agence nationale de la sécurité des systèmes d'information (ANSSI)** pour protéger les données des patients, des partenaires et des employés, est également un signe de **la volonté de l'établissement de prendre la sécurité informatique au sérieux**.

Il est important pour les organisations de disposer d'un plan de **cybersécurité efficace et de rester vigilant face à la menace croissante des cyberattaques**.



Centre Hospitalier de Nice

Le CHU Nice a failli être victime d'une cyberattaque le 15 décembre 2022. Cependant, grâce à ses **mesures de sécurité efficaces**, l'établissement a réussi à bloquer l'attaque avant qu'elle ne puisse causer des dommages importants. Selon les informations disponibles, **le pare-feu de l'établissement a réussi à empêcher toute intrusion dans le serveur de la messagerie de l'établissement**.

Grands comptes privés touchés

Groupe Leader

Le 2 février 2022, le Groupe Leader a été victime d'une cyberattaque. Celle-ci a été déclenchée par un **hameçonnage qui a visé un collaborateur de l'entreprise**. Suite à cette attaque, les données de l'entreprise ont été cryptées et supprimées, causant des perturbations importantes pour l'entreprise.

Le Groupe Leader est une entreprise spécialisée dans l'intérim qui compte 170 agences en Europe et emploie 13 000 intérimaires. L'attaque a eu lieu **pendant la période de paye de ces intérimaires**, rendant la situation encore plus critique. **Toutes les connexions aux systèmes de l'entreprise ont été bloquées**, ce qui a rendu impossible l'accès aux données et aux informations importantes pour l'entreprise.

Face à cette situation, le Groupe Leader a pris des mesures pour **renforcer sa sécurité informatique**. Il a **embauché un gestionnaire des risques** et a recouru à un **responsable de la sécurité des systèmes d'information (RSSI)** pour gérer les conséquences de l'attaque. Cependant, pour s'assurer d'une protection adéquate contre les cyberattaques à l'avenir, le Groupe Leader a également décidé de s'adoindre les services d'un prestataire de cybersécurité.



Selon Christophe Benoist, le directeur des systèmes d'information (DSI) du Groupe Leader, « Par crainte de ne pouvoir nourrir intellectuellement à plein temps ce RSSI, nous passons par un prestataire de cybersécurité avec qui nous avons signé la semaine dernière ». Cette démarche montre que l'entreprise **prend cette cyberattaque très au sérieux** et qu'elle met en place des mesures pour éviter que cela ne se reproduise à l'avenir.

Toyota

Le 28 février 2022, Toyota, le leader mondial de l'automobile, a été victime d'une cyberattaque **par le biais de son sous-traitant Kojima Industries**. Dans un communiqué, Kojima Industries a expliqué avoir détecté "un message de menace" samedi dernier avant de découvrir que son serveur informatique avait été "infecté par un virus". Il s'avère que la cyberattaque aurait pris la **forme d'un rançongiciel**.

En raison de cette attaque, Kojima Industries a décidé de **suspendre temporairement** lundi soir pour toute la journée de mardi dans ses **14 usines dans le pays**, affectant ainsi la production d'environ 13 000 véhicules.

Cette interruption de la production a causé **des perturbations significatives pour Toyota et ses clients**.



In extenso

Le 10 avril 2022, In extenso, une société française, a été victime d'une cyberattaque qui a paralysé son activité. Les pirates informatiques ont **utilisé un rançongiciel, REvil**, pour **soutirer "quelques millions d'euros"** à la société. La téléphonie de certaines de ses 250 agences en France a également été affectée par cette attaque.

Grands comptes privés touchés

Uber

Le 16 septembre 2022, Uber, le leader mondial des services de VTC, a été victime d'une cyberattaque de grande ampleur. Les pirates informatiques ont réussi à **compromettre un grand nombre de systèmes informatiques d'Uber**, obligeant l'entreprise à **mettre ces derniers hors ligne pendant plusieurs heures**.

Selon les enquêteurs, l'incident aurait débuté avec le **piratage d'un sous-traitant d'Uber**. Le cybercriminel aurait **acheté des données sur le darknet** avant d'utiliser un logiciel malveillant pour **accéder à l'ordinateur de ce sous-traitant**. Il aurait ensuite tenté de se connecter à son compte Uber à plusieurs reprises, jusqu'à ce que le **sous-traitant valide le second facteur push** pour stopper le spamming.

Grâce à cette première brèche, le hacker aurait pu accéder à de nombreux autres comptes d'employés d'Uber et **compromettre des applications cruciales pour l'entreprise, comme Slack ou les logiciels de facturation**.

Les enquêteurs suspectent que l'auteur de ces attaques soit un adolescent britannique de 17 ans, présumé membre du groupe Lapsus\$. Ces cyberattaques montrent à quel point il est important pour les entreprises de protéger leurs données sensibles et de sécuriser leurs systèmes contre les accès non autorisés, car la divulgation de telles informations peut causer des dommages considérables à la réputation de l'entreprise ainsi qu'à ses finances.

Rockstar Games

Le 19 septembre 2022, Rockstar Games, la société à l'origine de la célèbre franchise de jeux vidéo "Grand Theft Auto", a été victime d'une cyberattaque. Selon les enquêteurs, le **cybercriminel s'est introduit dans les serveurs de Rockstar Games** en utilisant la messagerie instantanée Slack et le logiciel de travail collaboratif Wiki Confluence.

En utilisant un code d'accès utilisateur, le hacker a pu accéder au serveur de Rockstar Games et **télécharger près de 90 millions de données**, ainsi que le code source de GTA 6, un jeu très attendu par les fans. En quelques minutes, des images que les créateurs du jeu avaient gardées secrètes depuis près de 5 ans **ont été divulguées sur le net**. Il a mis en vente sur le web le reste des données volées.

Metro

Le 17 octobre 2022, le groupe Metro a été victime d'une **cyberattaque de type DDoS** (Distributed Denial of Service). Cette attaque a **entraîné une panne informatique pendant plusieurs jours**, perturbant l'activité de l'ensemble des magasins du groupe.

Les pirates informatiques ont **pris en otage les systèmes informatiques de Metro**, ce qui a rendu difficile pour les professionnels de la restauration dépendants du groupe de s'approvisionner. Il est inconnu si des données ont été divulguées ou si une rançon a été versée.



Une attaque DDoS (Distributed Denial of Service) est une technique utilisée pour rendre un site web ou un service en ligne inaccessible en surchargeant les serveurs avec un grand nombre de demandes. Les attaques DDoS sont généralement lancées à partir de nombreux ordinateurs différents, appelés "zombies", qui ont été compromis par des logiciels malveillants et sont contrôlés à distance par un attaquant. Cela crée un grand nombre de requêtes simultanées qui peuvent rendre les serveurs inaccessibles pour les utilisateurs légitimes.

Les régions attaquées

Centre Val-de-Loire



Le 17 novembre, la Région Centre-Val de Loire a subi une tentative d'intrusion informatique via son site satellite de la Commission régionale. Pour prévenir tout risque pour les données, une dizaine de sites gérés par la collectivité ont été temporairement fermés.

Selon Alexandre Tinseau, responsable de la sécurité informatique de la Région, il n'y a pas lieu de s'inquiéter. Il a déclaré que "Il n'y a pas eu de demande de rançon. Ce n'est pas une attaque comme on a pu le voir sur des hôpitaux ou d'autres collectivités. C'est une tentative d'intrusion qui a échoué, parce qu'on a eu les bons réflexes"

Guadeloupe



Le 21 novembre, le Conseil régional de la Guadeloupe a annoncé avoir subi une cyberattaque de grande ampleur. Pour protéger les données, tous les réseaux informatiques ont été immédiatement interrompus.

La Direction des systèmes d'information est en contact étroit avec plusieurs autorités pour gérer cette situation : la Commission Nationale de l'Informatique et des Libertés (CNIL), l'Agence nationale de la sécurité des systèmes d'information (ANSSI), la Police nationale et la gendarmerie.

Normandie



La cyberattaque qui a touché la région Normandie le 9 décembre a eu pour conséquence la **paralysie des services informatiques du conseil régional**. À la suite de cette attaque, la Direction du Numérique de la collectivité a pris les mesures nécessaires pour caractériser et analyser le niveau de cette attaque ainsi que ses conséquences. Pour cela, elle a fait appel à une société spécialisée en cyberattaque.

La Région a également pris contact avec les services de l'Etat, l'**ANSSI** et les services de police afin de déposer plainte. **Les accès internet ont été suspendus sur les sites administratifs régionaux** de Caen et Rouen, dans les lycées, ainsi que dans certains des satellites de la collectivité.

Malgré ces perturbations, la Région a **rapidement réagi pour continuer à communiquer** avec les Normands. Le site internet de la Région a pu être restauré à une nouvelle adresse et de nouvelles adresses mails ont été attribuées.

Les départements touchés

CIG Grande couronne

Le 28 janvier, le Centre Interdépartemental de Gestion (CIG) Grande Couronne, **une administration conjointe à plusieurs départements d'Île-de-France**, a été victime d'une attaque informatique par **un rançongiciel**. Cette cyberattaque a rendu de nombreux services inaccessibles, notamment le site internet www.cigversailles.fr et les outils qui en dépendent, ainsi que le site du PASS Territorial. Les boîtes mails des collaborateurs ont également été perturbées.

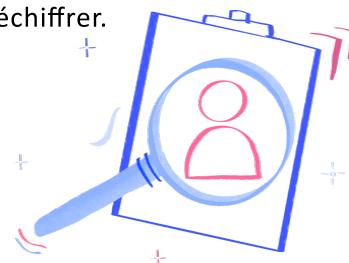
La Cnil (Commission nationale de l'informatique et des libertés) a été alertée ainsi que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et une enquête a été confiée aux gendarmes. Le CIG a mandaté une entreprise spécialisée, **Orange Cyberdefense**, pour gérer la crise et s'est appuyé sur les services d'un cabinet d'avocats et d'une société de communication.

A posteriori, le CIG a pu utiliser son assurance pour gérer la crise. Celle-ci a également été l'occasion pour l'établissement public de remettre à plat son architecture informatique. **Le CIG a changé de stratégie en matière d'hébergement de données en les répartissant entre de nombreux sites pour éviter une concentration de risques.**

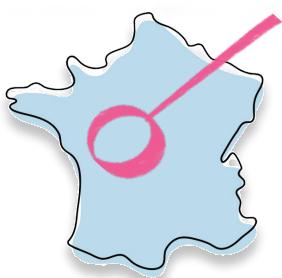
Ardèche

Le 6 avril, le département de l'Ardèche a été victime d'une cyberattaque menée par le groupe de **cybercriminels Lockbit 2.0**. Les serveurs du département ont été **touchés par un ransomware**, un type de logiciel malveillant qui chiffre les fichiers et exige une rançon pour les déchiffrer.

L'ultimatum expirait le 12 avril, faute de paiement, les pirates ont mis leurs menaces à exécution en **publiant sur le darkweb des milliers de fichiers dérobés** sur le serveur de la collectivité. Le groupe menaçait de dévoiler 40 000 fichiers ou documents, mais il n'est pas clair combien de données ont été finalement publiées.



Indre-et-Loire



Le 11 juillet, le département de l'Indre-et-Loire a été victime d'une cyberattaque qui a gravement paralysé son système informatique. Pour éviter la propagation d'un **assaut déclenché par des pirates confirmés**, la collectivité a été contrainte à reconstruire l'ensemble de son réseau informatique.

La veille, la majorité des installations informatiques était corrompue, avec environ 250 serveurs touchés par le logiciel malveillant, soit l'équivalent des trois quarts des serveurs utilisés par le Département. Les experts de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la cellule de cybercriminalité du ministère de l'Intérieur **ont travaillé plusieurs semaines pour identifier la faille et l'origine de l'infection.**

Bien que l'information n'ait pas encore été confirmée, il est question d'une probable hypothèse d'un **rançongiciel qui aurait été utilisé pour la cyberattaque**.

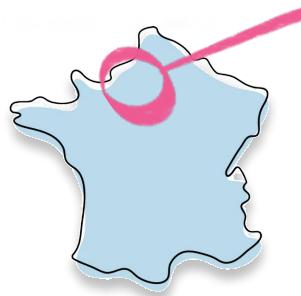
Les départements touchés

Alsace

Le 28 septembre, la Collectivité européenne d'Alsace (CEA) a été victime d'une cyberattaque. Selon les informations, **plusieurs services ont été touchés**. La direction de la CEA assure avoir réagi à temps et garantit qu'il n'y a eu aucune fuite de données.

La CEA a déposé plainte pour cette attaque et la cellule de cybercriminalité est chargée de l'enquête. Il a été indiqué que l'**adresse du pirate aurait été identifiée**.

Seine-Maritime



Le 10 octobre, le département de la Seine-Maritime a été victime d'une cyberattaque importante qui a **perturbé de nombreux services pendant plusieurs semaines**. Pour protéger les données et isoler son système informatique, la collectivité a dû **provisoirement couper complètement ses réseaux informatiques**.

Heureusement, les lignes téléphoniques du département ont été épargnées. Les espaces informatiques des collèges, les directions des routes, de l'environnement et les sites et musées départementaux ont pu être maintenus car **ils se trouvent sur un autre réseau que celui du département**.

Cependant, il était impossible d'effectuer certaines procédures dématérialisées, le fonctionnement du site était dégradé et **le département a mis plusieurs semaines pour avoir un retour à la normale**.

Seine-et-Marne

Le Dimanche 6 novembre 2022, le département de Seine-et-Marne a été victime d'une cyberattaque. **Les pirates ont exigé une rançon de 10 millions d'euros**. Les conséquences de cette attaque ont été significatives, les quatorze Maisons départementales de solidarités (MDS), les centres de protection maternelle et infantile (PMI) et les cinq musées départementaux tels que le musée Préhistoire d'Île-de-France ou le musée Stéphane Mallarmé étaient **devenus enjoignables par téléphone**. De même pour le château de Blandy-les-Tours qui n'était plus en mesure de prendre des réservations. Les 5 000 agents territoriaux ont également été affectés par la cyberattaque.

Pour faire face à cette situation, les agents ont **continué de travailler mais "à l'ancienne"**, c'est-à-dire en utilisant des papiers ou des téléphones portables mis à disposition pour pallier les numéros fixes désormais inutilisables. En raison de cette cyberattaque, le vote du budget avait été repoussé au début de l'année 2023.



Les départements touchés

Alpes-Maritimes

Le 9 novembre dernier, le Département des Alpes-Maritimes a été victime d'une cyberattaque **utilisant un rançongiciel**. L'opération a été revendiquée par le collectif Play. Le lendemain, les premières nouvelles de cette attaque ont commencé à se répandre.

Pour protéger les données et isoler son système informatique, tout le système informatique de la Collectivité a été coupé. Cette cyberattaque a été rapidement stoppée par les experts de la Direction des Services Numériques (DSN) de la Collectivité qui ont immédiatement déclenché une cellule de crise pour éviter la propagation du virus.

La DSN a travaillé en collaboration avec Orange Cyberdéfense et avec l'aide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Un diagnostic global de l'attaque a été rapidement posé : **282 Go ont été exfiltrés des serveurs du Département, ce qui correspond à 0,1% des données de l'administration.**

Heureusement, l'ensemble des données sont restées protégées : les dossiers des usagers des services départementaux n'ont pas été piratés. Les données dérobées concernaient essentiellement des données bureautiques et/ou des informations appartenant à des agents de la Collectivité. Les pirates ont publié les données exfiltrées sur internet mais avec l'aide d'Orange Cyberdéfense, **tous les fichiers ont pu être supprimés de la plateforme d'hébergement.**



Les communes de plus de 5 000 habitants ciblés

Montesquieu

La communauté de communes de Montesquieu a subi une cyberattaque le 13 mars dernier, qui a bloqué les employés de 13 communes de Gironde. Les services informatiques ont été paralysés, ne permettant plus l'accès aux courriels et aux fichiers. Cette attaque a perturbé le fonctionnement de la communauté de communes et une plainte a été déposée en gendarmerie.

Pour remédier à cette situation, la communauté de communes de Montesquieu a immédiatement mis en place un plan de reprise d'activité pour relancer les serveurs dès que possible et en toute sécurité. En parallèle, la collectivité s'est rapprochée de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour connaître la procédure à appliquer pour gérer ce type d'incident. Cette attaque montre l'importance de la sécurité informatique pour les collectivités territoriales et la nécessité de protéger les données sensibles des citoyens.

Aix-les-bains

La ville d'Aix-les-bains a subi une cyberattaque le 22 mars dernier, qui a paralysé l'ensemble de ses services. Selon les premières informations, **les serveurs de la ville auraient été utilisés pour miner des cryptomonnaies**.

Les agents de la mairie ont réussi à reprendre le contrôle de la situation et à rendre le système informatique opérationnel à nouveau. Cependant, la mairie a pris des mesures pour renforcer la sécurité de son réseau informatique pour éviter de futures attaques. La ville a également **déposé une plainte pour enquêter sur les auteurs de cette cyberattaque et pour évaluer les dégâts causés par cette attaque**.



Saumur

La ville de Saumur a été victime d'une cyberattaque le 23 mars dernier. Les conséquences ont été importantes, avec **des paralysies dans le système informatique de la ville**. Malgré cela, la mairie a rassuré la population en indiquant qu'aucune donnée n'a été extirpée.

Pour faire face à cette situation, la Ville a activé son plan de sauvegarde informatique et a créé une cellule de crise dédiée sous la direction de Jackie Goulet, Président-Maire. L'Agence Nationale de Sécurité du système d'information (l'**ANSSI**), la société **CAPGEMINI** et la Commission Nationale de l'Informatique et des Libertés (**CNIL**) ont également été saisies. Le coût total de la **récupération des données s'élève pour l'instant à 200 000 €**, sans avoir cédé aux demandes de rançon.

Les communes de plus de 5 000 habitants ciblés

Redon

La ville de Redon a été la cible d'une cyberattaque le 25 mai dernier. **Les services informatiques de l'administration ont réussi à stopper l'infection rapidement**, grâce à des outils de protection efficaces et à l'intervention rapide de l'équipe opérationnelle dirigée par la Direction des systèmes d'information (DSI).



La tentative de cyberattaque avait été organisée à travers **des comptes d'Office 365 de Microsoft piratés**, et **un agent de la ville de Redon agglomération avait été utilisé à son insu pour envoyer des mails frauduleux à son carnet d'adresses**.

Malgré cela, seulement 10 agents avaient été affectés et le fonctionnement des services de Redon agglomération n'a été **que temporairement ralenti**. La ville se félicite aujourd'hui de la réactivité de son service informatique et de l'absence de dommages significatifs.

Faulquemont

La cyberattaque qui a visé la ville de Faulquemont, le District urbain de Faulquemont (DUF) et le syndicat des eaux de Basses-Vigneulles et Faulquemont (SIEBF), le 10 juin dernier, **a été revendiqué par le groupe de hackers Lockbit**. Les serveurs informatiques des trois collectivités ont été gravement paralysés, entraînant une forte perturbation des activités des services municipaux.

La demande de rançon qui a accompagné l'attaque a ajouté **une pression supplémentaire sur les équipes de la ville**, qui ont dû agir rapidement pour limiter les dégâts. Les techniciens ont travaillé d'arrache-pied pour éviter la perte de données importantes, même les disques durs ont été touchés.

Finalement, après quatre jours d'efforts acharnés, les données ont pu être récupérées avec succès pour le District urbain de Faulquemont, la ville de Faulquemont et le syndicat des eaux. La ville de Faulquemont a réussi à limiter les dégâts de cette attaque informatique grâce à une réaction rapide et efficace, permettant ainsi de **maintenir les services essentiels pour les habitants**.

Guingamp

La ville de Guingamp a subi une cyberattaque en juin dernier, qui a **affecté deux de ses serveurs et causé une perte de données dans ses archives numériques** le lundi 4 juillet 2022. Bien que la collectivité ait réussi à récupérer les données perdues grâce à l'aide de sociétés spécialisées, il restait encore beaucoup de travail manuel pour les agents de la ville. **La facture totale s'est élevée à 18 500 €**. Heureusement, la ville n'a pas eu besoin de payer de rançon, car **l'email de demande de rançon a été pris pour un spam et supprimé**. Pour se protéger davantage contre de futures attaques, la ville de Guingamp a mis à jour son système d'exploitation en passant de Windows 7 à Windows 10.

Les communes de plus de 5 000 habitants ciblés

Maison-Alfort

La ville de Maison-Alfort a été la cible d'une cyberattaque le 27 septembre 2022. Les pirates informatiques ont réussi à **bloquer le réseau Internet et téléphonique** ainsi que le Portail Citoyen de la commune. Cette attaque a eu un impact considérable sur les services municipaux, **entraînant une paralysie de leur activité**.

Les citoyens de Maison-Alfort ont été invités à se rendre dans les accueils physiques des différents services municipaux pour toute démarche administrative. Il est à noter que cette ville a **déjà subi une attaque similaire en 2020**, ce qui montre la nécessité pour les communes de renforcer leur sécurité informatique face à ces menaces croissantes.

Caen

Le 26 septembre dernier, la ville de Caen a été victime d'une cyberattaque par **rançongiciel**. Les pirates informatiques ont tenté de s'introduire dans les systèmes informatiques de la ville, mais heureusement, **une technologie de détection de menace fournie par la société Harfang a permis de contenir les dégâts**. Cependant, tous les serveurs informatiques de la ville ont été coupés pour éviter toute propagation de la menace.

Malheureusement, cette attaque a eu des conséquences sur les services de la ville, notamment l'état civil. Heureusement, les données de la collectivité ne semblent pas avoir été affectées par cette attaque. **Aucune rançon n'a été demandée**.

La ville de Caen a immédiatement pris des mesures pour protéger ses systèmes informatiques et a porté plainte pour enquêter sur l'origine de cette attaque. Malgré ces efforts, le site internet de la ville n'est toujours pas accessible en janvier 2023. La ville travaille activement pour rétablir ses services et garantir la sécurité de ses données.

Les Mureaux

Le 24 septembre 2022, la ville des Mureaux a été victime d'une cyberattaque qui a **paralysé sa mairie**. Heureusement, l'intervention rapide des services municipaux a permis de stopper l'attaque. Cependant, en raison des risques potentiels, la ville a été contrainte de **restreindre fortement son accès aux serveurs et à Internet**.

Pour informer les citoyens, un message a été affiché sur le site internet de la ville, indiquant les services auxquels ils devaient se tourner pour les tâches administratives. Selon la ville, l'impact sur les habitants est très limité, la problématique étant plutôt interne, où les agents n'ont pas accès aux outils informatiques. **Une enquête de la DGSI est en cours** pour déterminer les circonstances de cette attaque et identifier les responsables.

Les communes de plus de 5 000 habitants ciblés

Brunoy

Le 29 octobre, la commune de Brunoy en Essonne a été victime d'une cyberattaque par un **groupe de hackers connu sous le nom de Lockbit 3.0**. Les pirates ont utilisé un **ransomware** pour crypter les données de la commune et ont exigé une rançon de 5 millions d'euros pour les déchiffrer.

Après cette attaque, de nombreux services municipaux ont été paralysés, et la mairie a dû mettre en place une stratégie de sécurité pour protéger les données et évaluer l'impact de l'attaque. Une plainte a été déposée et l'Agence nationale de la sécurité des systèmes d'informations (**ANSSI**) est en train d'enquêter sur les dégâts causés.

La somme exigée par les pirates est considérée comme astronomique pour une commune de 26 000 habitants. **Les groupes Lockbit 3.0 sont connus pour leur habileté à pénétrer les systèmes informatiques et pour leur utilisation de rançongiciels.** En juillet 2022, ils ont ciblé de nombreuses entreprises, dont le Centre Hospitalier de Corbeil-Essonnes, la ville de Westmount, des cabinets d'expertise comptable, l'Office d'Equipement Hydraulique de Corse et la ville de Faulquemont.

Frontignan

La cyberattaque subie par la commune de Frontignan la Peyrade a été un rude coup pour l'administration locale. Dans la nuit du mercredi 26 au 27 octobre, **des pirates informatiques ont réussi à s'introduire dans le système informatique de la mairie, demandant une rançon pour restituer les données volées.**

Face à cette situation, la municipalité a pris la décision de ne pas céder aux exigences des hackers. Elle a immédiatement **porté plainte et l'affaire est désormais entre les mains de la police judiciaire de Montpellier**, qui traite cette affaire via son pôle cybercriminalité.

Les conséquences de cette cyberattaque sont malheureusement lourdes pour la commune. **Les messageries et le site internet étaient paralysés**, et il était impossible d'effectuer les démarches administratives courantes telles que la réservation de crèche ou de cantine, les opérations financières ou de mandattement. De plus, **une semaine de données ont été perdues, ce qui peut causer de nombreux désagréments pour les administrés.**

Chaville

La ville de Chaville a **rapidement pris des mesures pour limiter les dégâts** causés par la cyber attaque qu'elle a subit dans la nuit du vendredi 14 au samedi 15 octobre 2022. Elle a immédiatement coupé l'accès à ses systèmes informatiques pour protéger les données et isoler le système des attaquants. **La mairie a travaillé en étroite collaboration avec des experts en cybersécurité pour évaluer l'ampleur de l'attaque et identifier les vulnérabilités.**

La mairie a également alerté les autorités compétentes, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI), pour obtenir une aide supplémentaire dans la gestion de la crise. Les investigations menées par les experts en cybersécurité ont révélé que l'attaque était le fait d'**un groupe de hackers connu sous le nom de Cuba Ransomware**.

Malgré les difficultés causées par cette attaque, la mairie de Chaville a réussi à **maintenir un certain niveau de service pour les administrés**. Les services municipaux tels que les crèches et les cantines ont continué à fonctionner normalement, et le site internet de la mairie est resté accessible. Toutefois, il est clair que la situation a été difficile pour les employés municipaux et les élus, qui ont dû travailler sans accès à leur boîte mail ou à d'autres outils informatiques.

Les communes de plus de 5 000 habitants ciblés

Sens

La ville de Sens, située dans l'Yonne, a été touchée par une cyberattaque les 5 et 6 mars derniers. Les détails de l'attaque sont peu connus, cependant, la Ville a pris des mesures immédiates pour bloquer les logiciels visés et mettre en place des actions préventives.

Cependant, malgré les efforts déployés pour contenir l'incident, la Ville demeure vigilante pour parer toute nouvelle menace potentielle. Il est important de noter que la cybersécurité est un enjeu majeur pour les collectivités, et il est crucial de continuer à renforcer les mesures de protection pour éviter de futurs incidents de ce type.

Rives de Moselle

La Communauté de communes Rives de Moselle a été victime d'une cyberattaque le 4 mars, lorsque des pirates informatiques ont utilisé un rançongiciel pour crypter l'ensemble des données informatiques de l'intercommunauté. Les employés ont été bloqués dans leur travail et il a été impossible d'accéder aux informations importantes.

La collectivité a immédiatement pris les mesures nécessaires pour limiter les dégâts causés par cette attaque. Une plainte a été déposée à la Gendarmerie de Maizières-lès-Metz et les signalements appropriés ont été réalisés auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) et de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

La Communauté de communes Rives de Moselle a également mis en place un plan de reprise d'activité pour relancer les serveurs dès que possible et en toute sécurité. Les employés et les élus sont restés vigilants pour éviter toute nouvelle menace. Malgré cette attaque, la Communauté de communes Rives de Moselle a réussi à protéger les données de ses citoyens et à maintenir le fonctionnement de ses services essentiels.

Saint Cloud

Le 21 janvier, la ville de Saint Cloud a été victime d'une cyberattaque qui a perturbé les services informatiques de la commune. Les pirates ont réussi à s'introduire dans notre système et ont exigé une rançon, menaçant de diffuser des informations volées si celle-ci n'était pas payée.

La Ville de Saint Cloud a pris la décision de ne pas céder à ce chantage et de ne pas financer le cybercrime. Nous avons donc refusé de payer la rançon. Malgré cela, les cybercriminels ont diffusé certains documents internes à la ville le 10 février.

La plupart des informations volées étaient déjà publiques ou obsolètes, comme des documents de travail datant de plusieurs années, des conventions avec des associations ou des délibérations et rapports du Conseil Municipal. Cependant, quelques informations confidentielles, telles que celles relatives à la gestion de la crise sanitaire, au CCAS ou à l'activité de la Police Municipale, ont également été dérobées.

Les fichiers contiennent essentiellement des coordonnées telles que le nom, prénom, date de naissance, adresse postale, numéro de téléphone et adresse e-mail de 391 personnes.

La ville de Saint Cloud a pris des mesures pour limiter les dégâts et renforcer la sécurité de ses systèmes informatiques, tout en restant vigilante face à toute nouvelle menace.

Sources

La Nouvelle République

France Bleu

Saint Nazaire News

RTL

Département 06

France3 Régions

Le Télégramme

Ouest-France

Actu

Le Parisien

France Info

20 minutes

Zataz

Pour connaitre d'autres territoires Française attaquées en 2022 : [ici](#)

