# Alerte : Comptes Twitter piratés. Comment les pirates ont fait et comment vous en protéger ?


Alerte : Comptes Twitter piratés. Comment les pirates ont fait et comment vous en protéger ?

**De nombreux comptes, dont celui du ministère français de l'Economie, ont été piratés, mercredi matin, par un message évoquant le référendum constitutionnel du 16 avril en Turquie.**

*« #Allemagne nazie #Pays-Bas nazis. Voici une petite claque ottomane pour vous. »* Mercredi 15 mars au matin, de nombreux comptes Twitter de personnalités et d'institutions ont publié un message, débutant par une croix nazie, évoquant le référendum constitutionnel du 16 avril en Turquie.

Parmi les victimes de ce piratage massif et hautement politique se trouvent :
• Le Ministère français de l'Economie,
• Le journal économique Forbes,
• Le Monde,
• Le site d'Alain Juppé,,
• le magazine « Envoyé spécial »,
• L'Académie de Rennes,
• Reuters au Japon,,
• le compte de l'émission « Envoyé Spécial »,,
• Nike en Espagne,,
• Unicef USA,,
• la Philharmonie de Berlin,
• Comptes d'université américaine…

Le compte Twitter officiel de Bercy a été piraté mercredi 15 mars. (CAPTURE D'ÉCRAN)

## Comment les pirates ont procédé

Pour réussir cette opération, le ou les pirates n'ont, a priori, pas eu recours à un système de détournement de mots de passe des comptes Twitter concernés. La faille provient, en fait, d'une « application tierce » : Twitter Counter, un outil payant et indépendant du réseau social. En échange d'une autorisation d'accès au compte, cette application propose aux entreprises et institutions des statistiques avancées, comme un suivi détaillé du nombre d'abonnés.
L'application Twitter Counter a confirmé, mercredi matin, le piratage de son service, et a annoncé le lancement d'une enquête interne. Dans un message posté sur le réseau social, l'entreprise rappelle qu'elle ne conserve pas les mots de passe de ses clients et assure qu'elle a désormais bloqué l'option qui lui permettait de poster des messages sur le compte de ses clients.
Cette méthode de piratage ne concerne malheureusement pas seulement les comptes Twitter d'importance. Si vous êtes un adepte du réseau social, vous avez sans doute déjà été tenté d'installer une application tierce vous permettant, par exemple, d'identifier les utilisateurs qui ont cessé de suivre votre compte. Celles-ci, comme Twitter Counter, ont de grandes chances de pouvoir publier des tweets en votre nom.

## Comment savoir si votre compte est vulnérable

Pour vérifier l'identité des programmes tiers ayant accès à votre compte, rendez-vous dans la catégorie « Applications » des paramètres de Twitter. Vous trouverez une liste de tous les programmes tiers que vous avez installés, ainsi que les différents niveaux d'autorisations d'accès de ces applications à votre compte.
Si vous voyez l'application « Twitter Counter » dans cette liste, cliquez sur le bouton « Révoquer l'accès » en face d'elle.
Si certaines vous semblent farfelues ou peu sûres, vous pouvez également les signaler auprès de Twitter en cliquant sur « Signaler l'application » après avoir révoqué leur accès à votre compte.
Dans l'exemple ci-dessous, l'application Periscope est ainsi autorisée à lire uniquement des tweets, Vine à lire et à publier, et Tweetdeck à lire, publier, et accéder aux messages privés.


## Notre avis

Je pense qu'il est anormal qu'une application tierce à Twitter comme « Twitter Counter » ait des droit d'écriture directement sur les comptes Twitter de ses abonnés ?
Pour ceux qui ne le savent pas, Twitter Counter permet d'analyser l'évolution de votre compte Twitter en « nombre de tweets, d'abonnés, de retweets et de mentions ».
Pourquoi une telle application à imposé à ses utilisateurs de pouvoir écrire sur leur compte ? Un simple droit en lecture est suffisant pour connaître le nombre d'abonnés, de tweets, retweets…
Partez à la chasse aux applications intrusives en vous rendant dans :
**Twitter > Paramètres et fonctionnalités > Applications**
et n'hésitez pas à « **Révoquer l'accès** » pour chacune des applications suspectes.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Twitter : comment Bercy et d'autres comptes officiels ont été piratés (et comment vous en protéger)*

---

# Arnaques entre cybercriminels !

| | |
|---|---|
|  | **Arnaques entre cybercriminels !** |

---

**Les chercheurs de Kaspersky Lab ont découvert PetrWrap, une nouvelle famille de malware exploitant le module d'origine du ransomware Petya et distribuée via une plate-forme RaaS (Ransomware as a Service) pour mener des attaques ciblées contre des entreprises. Les créateurs de PetrWrap ont produit un module spécial qui modifie le ransomware Petya existant « à la volée », laissant les auteurs de ce dernier impuissants face à l'utilisation non autorisée de leur propre malware. Ce pourrait être le signe d'une intensification de la concurrence sur le marché souterrain du ransomware.**

En mai 2016, Kaspersky Lab avait découvert le ransomware Petya, qui non seulement chiffre les données stockées sur un ordinateur mais écrase aussi le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées. Ce malware est un modèle de RaaS (Ransomware as a Service), c'est-à-dire que ses créateurs proposent leur produit malveillant « à la demande », afin de le propager via de multiples distributeurs en s'octroyant un pourcentage des profits au passage. Pour s'assurer de recevoir leur part du butin, les auteurs de Petya ont inséré certains « mécanismes de protection » dans leur malware de façon à prévenir un usage non autorisé de ses échantillons. Les auteurs du cheval de Troie PetrWrap, dont les activités ont été détectées pour la première fois au début de 2017, sont parvenus à contourner ces mécanismes et ont trouvé un moyen d'exploiter Petya sans verser de redevance à ses auteurs.

Le mode de diffusion de PetrWrap reste à éclaircir. Après infection, PetrWrap lance Petya afin de chiffrer les données de sa victime, puis exige une rançon. Ses auteurs emploient leurs propres clés de chiffrement privées et publiques en lieu et place de celles fournies avec les versions « standard » de Petya. Cela leur permet d'exploiter le ransomware sans avoir besoin de la clé privée d'origine pour décrypter la machine de la victime, dans le cas où cette dernière paie la rançon…[lire la suite]

---



Réagissez à cet article

Source : *PetrWrap : des cybercriminels volent le code de ransomware d'autres criminels Le nouveau ransomware mène des attaques ciblées contre des entreprises – Global Security Mag Online*

---

# Les messages de WhatsApp peuvent être facilement lus par la CIA


Les messages de WhatsApp peuvent être facilement lus par la CIA

---

**L'organisation WikiLeaks a reçu une importante base de données révélant les techniques de cyber-surveillance et de piratage de la CIA. Selon ces informations l'agence de renseignement américaine peut facilement accéder aux messageries, y compris WhatsApp et Telegram.**

La Central Intelligence Agency (agence centrale de renseignement, CIA) est capable de contourner le cryptage de certaines applications populaires de messagerie, y compris WhatsApp et Telegram, selon les documents publiés par WikiLeaks aujourd'hui.
« Ces techniques permettent à la CIA de contourner le cryptage de WhatsApp, de Signal, de Telegram, de Wiebo, de Confide et de Cloackman en piratant les téléphones « intelligents » sur lesquels ces applications sont installées et de collecter les enregistrements audio et les messages avant que le cryptage ne soit activé », informe le document publié par WikiLeaks.


© FLICKR/ VIN CROSBIE
Espionnage en plein ciel: Air France dans le viseur des services secrets US et UK

Cette fuite a semé le trouble parmi les utilisateurs de WhatsApp, dont beaucoup ont réagi avec virulence aux nouvelles selon lesquelles l'application aurait commencé à partager des données avec Facebook l'année dernière.
La révélation de WikiLeaks suggère que les espions du gouvernement américain ont eu accès aux messages des utilisateurs malgré la mise en place d'un cryptage de bout en bout, qui est pourtant conçu pour protéger la confidentialité des utilisateurs.
Cependant, il se pourrait que la CIA n'ait pas piraté les applications elles-mêmes, mais craqué les outils de cryptage en attaquant les smartphones des utilisateurs.


© AFP 2017 SAUL LOEB
WikiLeaks publie plus de 8.700 documents concernant les capacités de cyber-espionnage de la CIA

Le site de Julian Assange, WikiLeaks, a annoncé le 7 mars la publication d'une nouvelle série de fuites sur la CIA sous le code « Vault 7 » qui sera, d'après le communiqué de l'organisation, la plus importante publication de documents confidentiels sur l'agence.
La première partie des fuites, intitulée « Year Zero », comprend 8 761 documents et fichiers qui ont été collectés sur un réseau isolé de haute sécurité du Centre Cyber Intelligence (département de la CIA) à Langley, dans l'État de Virginie.
Les fuites de « Year Zero » révèlent les capacités de piratage de la CIA contre un large éventail de produits américains et européens, notamment Windows, iPhone, Android et même les téléviseurs Samsung, qui ont été transformés en microphones cachés par le programme Weeping Angel…[lire la suite]

---



Réagissez à cet article

Source : *Les messages de WhatsApp peuvent être facilement lus par la CIA*

---

# Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft


Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft

---

**Une vulnérabilité a été découverte dans les navigateurs Microsoft. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.**

# 1 – Risque(s)

• exécution de code arbitraire à distance

# 2 – Systèmes affectés

• Internet Explorer 11 pour Windows 7
• Internet Explorer 11 pour Windows 8.1
• Internet Explorer 11 pour Windows 10
• Internet Explorer 11 pour Windows Server 2012 et 2016
• Microsoft Edge pour Windows 10

# 3 – Résumé

Une vulnérabilité a été découverte dans les navigateurs Microsoft. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

# 4 – Contournement provisoire

Une vulnérabilité présente dans les navigateurs Internet Explorer et Edge permet à un attaquant d'exécuter du code arbitraire depuis une page internet malveillante.
Cette vulnérabilité exploite une faille de type confusion de type et peut être déclenchée en définissant des valeurs particulières pour les propriétés d'un objet tableau dans une page Web spécialement conçue.
On notera que cette vulnérabilité est atténuée par l'utilisation de la mesure de sécurité de Windows Control Flow Guard (CFG) au sein de l'application. Un attaquant souhaitant exploiter la vulnérabilité devra ainsi mettre en oeuvre un contournement de la contre-mesure CFG.
Aucun correctif n'est prévu par Microsoft avant la publication mensuelle des correctifs de sécurité du mois de mars. Dans l'attente de la disponibilité d'un correctif de sécurité, le CERT-FR recommande de privilégier l'utilisation de navigateurs autres qu'Internet Explorer ou Edge pour la navigation sur Internet.

# 5 – Documentation

• Rapport de Bogue de Project Zero du 23 février 2017
https://bugs.chromium.org/p/project-zero/issues/detail?id=1011
• Référence CVE CVE-2017-0037
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037
.

---



Source : *Vulnérabilité dans les navigateurs Microsoft*

# Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr


Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

**Yahoo donne les détails des hacks qui ont touché plus d'un milliard de comptes, et en révèle un nouveau. Et la patronne se serait fait sucrer ses primes.**

La crucifixion de **Yahoo** continue, et si ce n'est pas déjà fait, on ne peut que vous recommander à ce stade de supprimer votre éventuel compte Yahoo. Dans un communiqué, l'entreprise est revenue par le menu sur toutes les attaques qui ont gravement entaché la réputation de l'entreprise depuis 2014. On y apprend en prime que dernièrement, des hackers ont obtenu du code propriétaire de Yahoo et ont pu fabriquer de faux cookies.
Cela leur aurait permis d'accéder à 32 millions de comptes entre 2015 et décembre 2016. Sur cette masse, seuls 26 utilisateurs auraient été prévenus. L'entreprise explique également collaborer avec les autorités depuis que son enquête a révélé la possible implication de **hackers** soutenus par un état dans ces piratages. En tout, plus d'un milliard de comptes Yahoo ont été compromis depuis 2014…[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr*

# 1,2 million de francs détournés d’une entreprise Bernoise


1,2 million de francs détournés d’une entreprise Bernoise

**CYBERCRIMINALITÉ – Une société bernoise a été victime de piratage informatique. En tout, 1,2 million de francs ont été détournés. Le patron ne décolère pas, s'étonnant du manque de réactivité des banques.**

Des cyber-criminels sont parvenus à détourner 1,2 million de francs des comptes de la société bernoise Küng Holding. Mis à part 160'000 francs, l'argent a pu être récupéré, mais le patron de l'entreprise Christoph Küng ne décolère pas.

Ce dernier s'étonne d'une part que trois banques aient déclenché sans demande d'éclaircissements des paiements vers d'obscures adresses. Dans un cas, 785'000 francs ont notamment été versés à un individu au Kirghizistan. D'autre part, M. Küng estime que le logiciel de paiement utilisé comporte de sérieux problèmes de sécurité.

Ces failles ont rendu possibles les ordres de paiement du pirate informatique, a confié jeudi Christoph Küng à l'ats. Il confirmait des informations publiées par le site internet Inside Paradeplatz, le Bund et la Berner Zeitung.

## Cheval de Troie

Les cyber-criminels ont agi en utilisant le cheval de Troie Gozi, qui s'introduit dans les ordinateurs par le biais d'une pièce-jointe dans un courriel. Ces ordres de paiement ont seulement éveillé les soupçons de PostFinance, qui a considéré une demande de virement de 49'000 francs comme « inhabituelle ».

Les trois banques ont en revanche autorisé ces paiements sans difficulté. Ce n'est que par la suite que Christoph Küng a pu péniblement stopper une grande partie de ces virements et récupérer l'argent.

La société informatique suisse qui a développé le logiciel se défend des accusations, estimant que Küng Holding n'a pas installé une mise à jour importante. Christoph Küng nie toutefois cette affirmation…[lire la suite]

NDLR : Denis JACOPINI souhaiterai bien être Expert judiciaire désigné sur cette affaire. Analyser le moyen utilisé par le pirate informatique pour modifier le comportement du logiciel de comptabilité devrait être très instructif !

La responsabilité de l'éditeur va t-elle être recherchée en raison de l'existence d'une faille de sécurité sans son logiciel et en raison de sa possible négligence pour ne pas avoir mis en place des mesures de sécurité adapté au coté sensible de la fonction de virement automatique ?

La responsabilité du dirigeant qui n'a pas appliqué la mise à jour recommandée est elle engagée ?

Peut-être bien que l'expertise permettra d'aboutir à une toute autre cause .

Si nous le pouvons, nous suivrons cette affaire.

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Piratage informatique dans une entreprise bernoise: 1,2 million de francs détournés*

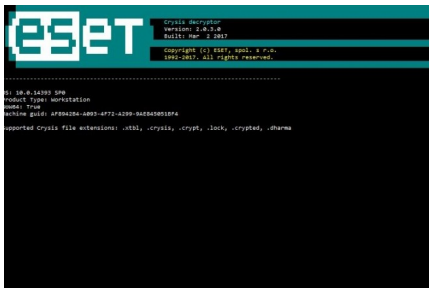
---

# Le Ransomware Dharma enfin décrypté


Le Ransomware Dharma enfin décrypté

---

**Les clés de déchiffrement du ransomware Dharma ainsi que toutes ses variantes ont été mises en ligne par un utilisateur. Kaspersky et Eset ont mis à jour leurs outils de lutte contre les ransomwares pour permettre à toute personne ou entreprise de déchiffrer gratuitement leurs fichiers chiffrés.**




Les fournisseurs de sécurité dont Kaspersky et Eset ont mis à jour leurs outils pour permettre de déchiffrer les fichiers piégés par le ransomware Dharma. (crédit : D.R.)

C'est une belle victoire qui vient d'être remportée contre le diabolique ransomware Dharma. Les personnes ayant des fichiers chiffrés par ce programme peuvent en effet souffler car ils peuvent désormais avoir accès à des clés de déchiffrement pour pouvoir les retrouver. Apparu pour la première fois en novembre, Dharma est basé sur l'ancien programme de ransomware Crysis. Il est facile de le reconnaitre par l'ajout aux fichiers chiffrés de l'extension .[email_address].dharma. , l'adresse mail correspondant à celle utilisée par le pirate pour tenter d'extorquer sa victime.
Mercredi, un utilisateur sous le pseudonyme de gektar a publié un lien vers un post Pastbin sur le forum du support technique de BleepingComputer.com. Un post indiquant contenir les clés de déchiffrement du ransomware Dharma et de toutes ses variantes. Etrangement, la même chose s'est produite en novembre avec les clés de son prédécesseur, Crysis ce qui a permis à des chercheurs de créer des outils de déchiffrement. Aucune autre motivation que celle de mettre à disposition ces clés n'a été enregistrée concernant gektar. La bonne nouvelle est que ce leak a permis aux chercheurs de Kaspersky et d'Eset de vérifier son travail. Bingo : les deux sociétés ont mis à jour leurs outils de déchiffrement respectifs à savoir RakniDecryptor et CrysisDecryptor.

## Une guerre des gangs dans les ransomwares

Cette situation devrait résonner à l'oreille des personnes touchées par des ransomwares qui ne devraient pas oublier de conserver une copie de leurs fichiers chiffrés à leur insu. Les chercheurs trouvent en effet parfois des failles dans les implémentations du chiffrement des ransomwares leur permettant de casser le chiffrement des clés. Dans d'autres cas, les autorités judiciaires et de police saisissent les serveurs de commande et de contrôle utilisés par les gangs de ransomware et publient ces clés.
Dans d'autres cas comme ici, les clés arrivent à la surface par d'autres moyens inexpliqués. Peut être parce que le développeur du ransomware a décidé de fermer boutique et décide de lâcher les clés, ou alors a-t-on à faire à une rivalité entre deux gangs de hackers qui se mettent des bâtons dans les roues pour court-circuiter l'activité des uns et des autres. Dans tous les cas, il est également recommandé de jeter un oeil sur le site NoMoreRansom.org, régulièrement mis à jour et proposant aussi bien des outils que des conseils pour lutter contre ces fichus ransomwares.

Article rédigé par Lucian Constantin / IDG News Service

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Un ransomware piège les Mac*

---

# Cybersécurité dans le monde : à quoi peut-on s'attendre ?


## Cybersécurité dans le monde : à quoi peut-on s'attendre ?

**L'année 2016 a démontré que les mesures de sécurité traditionnelles ne suffisaient plus et que de nouvelles stratégies devaient être mises en place. 2017 va donc s'inscrire dans la continuité de ce qui a déjà été amorcé l'année passée, à savoir : toujours plus de sécurité pour toujours une protection maximisée. Les experts de NTT Security ont fait ressortir les tendances et les prévisions pour cette année qui débute.**

Selon Garry Sidaway, Vice-Président Senior de la Stratégie de Sécurité

**1. L'identité restera au cœur des enjeux**

Au risque de nous répéter, les mots de passe fournissent aujourd'hui des garanties insuffisantes. À l'ère du digital et de la mobilité, commodité et sécurité ne font pas bon ménage. Certes, les mots de passe sont bien pratiques, mais ils sont de moins en moins perçus comme une preuve d'identité irréfutable. Devant l'utilisation croissante des smartphones et les exigences de simplicité des consommateurs et des professionnels, les solutions d'identité resteront donc au cœur des préoccupations en 2017. C'est ainsi que le mot de passe traditionnel cèdera du terrain face à la poussée du « multi-facteurs », une méthode combinant plusieurs facteurs d'authentification (localisation, possession d'un objet, d'une information, etc.). Cette association entre physique et digital, avec en toile de fond l'émergence de méthodes d'authentification avancées, favorisera le développement de nouvelles solutions de gestion des identités.

**2. Le mobile sera omniprésent**

Au royaume du digital, le mobile est roi. Un roi qui bouscule l'ordre établi dans de nombreux domaines, des méthodes de paiement jusqu'aux interactions sociales. Véritables hubs digitaux, nos smartphones constituent désormais non seulement une fenêtre de contrôle et d'interaction avec le monde mais aussi une interface d'identification et d'authentification. Dans un tel contexte, 2017 verra le curseur de la menace se déplacer des ordinateurs portables vers les appareils mobiles. Si, traditionnellement, les acteurs de la sécurité se sont concentrés sur les systèmes back-end et les conteneurs, ils devront revoir leur approche pour placer le mobile au cœur de leur dispositif.

**3. Les entreprises surveilleront la menace interne**

Le problème des menaces internes ne date pas d'hier. Côté défense, les progrès réalisés dans les domaines de l'analytique et de la détection des anomalies devraient se poursuivre en 2017. Dans un milieu de l'entreprise de plus en plus dynamique, définir les critères d'un comportement utilisateur « normal » restera un défi de taille. Toutefois, avec le développement de nouvelles techniques de machine learning, nous verrons l'analyse comportementale s'opérer directement au niveau des terminaux.

**4. Fin de la détection basée sur les signatures**

Antivirus nouvelle génération, solutions de sécurité des terminaux, solutions de détection et de réponse aux incidents… Peu importe leur nom, les solutions de protection des terminaux se projetteront bien au-delà de la détection basée sur des signatures statiques, à commencer par les outils d'analyses avancées que l'on retrouvera systématiquement sur ces solutions. Leur force résidera notamment dans leur capacité à exploiter la puissance du cloud pour partager l'information sur les menaces connues. La diversité et le volume sans précédent des malwares engendreront l'émergence d'une nouvelle approche. Destinée à enrayer le syndrome dit du « patient zéro », cette démarche reposera à la fois sur une collaboration internationale et l'utilisation d'une cyberveille prédictive et proactive pour libérer toute la force du collectif.

**5. Le tout-en-un fera de plus en plus d'adeptes**

Alors que le marché de la cybersécurité se consolide, les entreprises se tournent vers des solutions de sécurité couvrant l'intégralité des environnements TIC. Traditionnellement, la force des prestataires de sécurité managée (MSS) s'est située dans leur capacité à intégrer un maillage d'outils complexes et pointus. Aujourd'hui, la situation a changé. Tout l'enjeu consiste à intégrer le facteur sécurité à tous les échelons du cycle opérationnel de l'entreprise. Les clients chercheront donc un partenaire capable d'agir sur tous les fronts : applications métiers, infrastructure réseau, services cloud et de data center autour d'une console de gestion centralisée. En 2017, les solutions multifournisseurs apparaîtront comme datées. Les acteurs de la sécurité devront ainsi coordonner un service complet de bout en bout pour répondre aux enjeux de l'espace de travail digital.

Selon Stuart Reed, Directeur Senior Product Marketing

**6. Les consommateurs exigeront plus de transparence**

Une étude récente de NTT Security a mis en lumière les attentes croissantes des cyberconsommateurs en matière de transparence, tant sur le plan des pratiques que de la gestion des incidents. Ces conclusions traduisent notamment une sensibilisation accrue des consommateurs sur les questions de sécurité suite aux scandales de violations à répétition. La tendance est appelée à se poursuivre en 2017 et au-delà. Notons enfin que les entreprises dotées de politiques de sécurité et de plans d'intervention efficaces diminueront leur exposition au risque, tout en profitant d'un puissant levier de compétitivité.

**7. L'innovation en moteur de consolidation**

Du point de vue de l'offre comme des fournisseurs de cybersécurité, 2016 a été placée sous le signe de la consolidation. Au rang des plus grosses opérations, on citera l'acquisition de BlueCoat par Symantec, la série de rachats par Cisco et, plus proche de nous, la création de NTT Security autour de trois piliers : analytique de pointe, cyberveille avancée et conseils d'experts en sécurité. Derrière ce phénomène de consolidation, on retrouve une constante : l'innovation. Concrètement, les grandes entreprises ont racheté des spécialistes pour accéder à leurs compétences et les englober dans une offre plus aboutie. Ces grands acteurs profitent enfin d'économies d'échelle considérables – et de l'expertise et de l'efficacité qui en découlent – pour mener des programmes d'incubation qui viendront à leur tour stimuler l'innovation. Cette tendance de fond souligne bien l'importance de l'innovation pour évoluer au rythme des besoins de sécurité des clients.

**8. L'identité des objets**

Avec l'essor de l'IoT, la frontière entre physique et digital s'estompe peu à peu pour créer des expériences clients plus pratiques, rapides et efficaces. Seulement voilà, les cybercriminels ont eux aussi investi la sphère de l'IoT à l'affût de la moindre vulnérabilité. On a ainsi recensé des cyberattaques se servant d'objets connectés (caméras de vidéosurveillance, imprimantes…) pour lancer des attaques DDoS qui sont parvenues à paralyser des sites comme Twitter et Spotify. L'année 2017 verra sans doute une recrudescence des attaques perpétrées à l'encontre des objets connectés. D'où le besoin impérieux d'intégrer ces appareils à une politique de sécurité plus complète, notamment pour mieux contrôler l'identité et la légitimité de leurs utilisateurs.

**9. L'analytique changera la donn**

L'un des grands défis de la cybersécurité pourrait se résumer par cette question : comment produire une information cohérente à partir d'une avalanche de données issues de dispositifs multiples ? Si l'analyse de données a pour fonction première de « donner du sens », l'évolution des menaces doit nous inciter à revoir nos méthodes d'interprétation et de contextualisation de l'information. Dans cette optique, les outils avancés d'analyse du risque vous permettront de prendre les bonnes décisions. Au-delà des événements présents, ces outils ont pour fonction de décortiquer les données historiques pour faire ressortir des tendances, mais aussi d'utiliser l'intelligence artificielle pour identifier les schémas comportementaux annonciateurs d'une attaque. Fondées sur des technologies avancées de machine learning, des outils d'analyse automatiques et des experts en astreinte permanente, les solutions d'analytique de pointe promettent de changer la donne dans le secteur des MSS.

Selon Kai Grunwitz, Vice-Président Senior Europe Centrale

**10. La cybersécurité va s'imposer comme un facteur clé de succès**

Pour être reconnue comme tel par tous les acteurs concernés, la cybersécurité doit s'intégrer en amont à l'ensemble des processus métiers de l'entreprise. Dans un monde connecté où le digital gagne chaque jour en importance, les entreprises veulent pouvoir compter sur une sécurité parfaitement incorporée à leurs stratégies métiers et IT. Outre son rôle indispensable de gardienne des données sensibles, du capital intellectuel et des environnements de production, la cybersécurité sera également partie intégrante de l'innovation et de la transformation de l'entreprise.

La sécurité ne sera plus seulement le problème des DSI, mais s'invitera au cœur des processus métiers et constituera l'un des ressorts de la chaîne de valeur. Enfin, la gestion du cycle de sécurité constituera un différenciateur clé autant qu'une priorité essentielle dans le cadre d'une stratégie de sécurité orientée métiers. Elle procurera aux entreprises un avantage concurrentiel et un réel levier de valeur ajoutée.

Selon Chris Knowles, Directeur solutions

**11. Le RGPD sera partout !**

Si vous pensiez que le Règlement général sur la protection des données (RGPD) a été l'un des grands thèmes de 2016, attendez de voir ce que 2017 vous réserve. Alors que les fournisseurs proclameront les avantages de leurs technologies et que les équipes juridiques plancheront sur la définition d'une sécurité réellement irréprochable, les clients, eux, se lanceront dans les préparatifs.

**12. Au royaume des aveugles, les borgnes sont rois… mais plus pour très longtemps !**

Pour beaucoup d'entreprises, la sécurité se résume à la protection d'un périmètre au moyen de périphériques inline censés analyser l'intégralité du trafic et intervenir sur la base d'éléments visibles. Toutefois, la mobilité croissante des collaborateurs, associée à l'explosion du nombre d'applications cloud en entreprise, créent des « angles morts ». À commencer par le transit d'informations via des tunnels cryptés, le stockage et le traitement de données à l'extérieur de data centers sécurisés, ou encore les communications entre machines virtuelles qui échappent totalement à la surveillance des dispositifs de sécurité existants. En 2017, les entreprises se pencheront sur ce phénomène afin d'éliminer les angles morts et de reprendre le contrôle de leur sécurité.

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Cybersécurité dans le monde : à quoi peut-on s'attendre ?*

---

# La commission de contrôle des élections veillera au 'risque d'attaque informatique'


---

**Saisir les autorités en cas de cyberattaque, veiller au respect du principe d'égalité entre les candidats à l'élection présidentielle… La Commission nationale de contrôle de la campagne a été installée ce soir au Conseil d'Etat par le ministre de la Justice.**

La commission portera « une vigilance particulière au risque d'attaque informatique de la campagne », a déclaré le garde des Sceaux Jean-Jacques Urvoas. En décembre, l'Agence nationale de la sécurité des systèmes d'information (Anssi) et le Secrétariat général de la défense et de la sécurité nationale (SGDSN) avaient souligné « le risque de cyberattaque à motif politique », a rappelé Jean-Jacques Urvoas.

**» Lire aussi : L'Élysée inquiet d'une cyber-menace étrangère pesant sur la présidentielle**

« Si un candidat estime qu'il fait l'objet d'une attaque susceptible d'affecter le déroulement de sa campagne, il pourrait saisir la commission », a confirmé son président Jean-Marc Sauvé, à la tête du Conseil d'Etat. Mais il revient d'abord aux candidats et à leurs partis politiques de « mettre en oeuvre les solutions adéquates » pour y faire face, a-t-il toutefois précisé. Si une attaque devait être avérée, la commission – en lien avec le Conseil constitutionnel – demanderait des investigations…[lire la suite]

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

---

## Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

---

Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;

• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

---

Contactez-nous

---

Source : *La commission de contrôle des élections veillera au ‘risque d’attaque informatique’*

---

# Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

---

**Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.**

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

**FOCUS**

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

## Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI
• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI
Notre dossier : Données personnelles, un gisement sous haute protection

## Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

## Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

## Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

## L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

---

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

---



Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*