LE JOURNAL DU DPO

Julia Garcia de Barros - Stéphane Riffard

juillet - août 2022 Vol. 16

DANS CE NUMÉRO

Un mot du DPO

L'actualité en bref :

- Publicité ciblée
- Data brokers
- Site web
- Sanction CNIL

Zoom sur :

La vision de la cybersécurité par les collectivités :
Une prise en compte inégale des risques informatiques

Contact :

service.dpo@manchenumerique.fr
Service DPO, Manche Numérique
235 rue Joseph Cugnot
50000 SAINT LO

UN MOT DU DPO

Bonjour tout le monde !
J'espère que vous allez bien.
Vous avez de nouveau droit à une édition spéciale pour cet été sachant que la plupart d'entre vous a prévu des vacances. Vous pourrez emmener les jeux pour la plage pour vous occuper !
Bonne lecture 😄

L'ACTUALITÉ EN BREF

Publicité ciblée : Tik Tok a suspendu la mise à jour de ses conditions d'utilisation en Europe sous la pression de la DPC (CNIL irlandaise). Cette mise à jour impose l'affichage de publicité ciblée sans demander au préalable le consentement de l'utilisateur en se basant sur l'intérêt légitime des annonceurs et des utilisateurs.

Data brokers : Ouverture d'une enquête de 15 mois par le laboratoire d'innovation numérique de la CNIL sur le business des data brokers. Sur la base d'échantillons, ils vont tester les possibilités de réidentification des personnes via la géolocalisation de leur identifiant publicitaire.

Site web : 15 mises en demeure ont été prononcées par la CNIL pour des sites web insuffisamment sécurisés dans le cadre de sa thématique de contrôle sur la sécurité des sites web. Des problèmes de chiffrement des données et de sécurisation des comptes utilisateurs ont été détectés.

Sanction CNIL : Sanction de Total énergies de 1 millions d'euros par la CNIL pour manquements concernant l'exercice des droits, notamment le droit d'opposition à la prospection commerciale et les réponses aux demandes de droit d'accès.

ZOOM SUR :

LA VISION DE LA CYBERSÉCURITÉ PAR LES COLLECTIVITÉS : UNE PRISE EN COMPTE INÉGALE DES RISQUES INFORMATIQUES

Nous entendons régulièrement parler d'attaques informatiques touchant des entreprises privées ainsi que des collectivités. Les collectivités sont des cibles intéressantes pour les pirates car elles sont essentielles pour réaliser les actes de la vie courante. Selon l'ampleur de l'attaque, un seul poste peut être touché comme tout le système d'information qui se retrouve paralysé. Les questions qui se posent sont de savoir comment les collectivités abordent cette problématique et comment les aider à faire face à ces attaques en prévenant les risques.

Constatations de l'enquête de Cybermalveillance.gouv :

Pour accompagner la transformation numérique des collectivités, le gouvernement a mis en place le plan France Relance comportant différents volets. Dans le cadre du volet relatif à la cybersécurité, Cybermalveillance.gouv a mené une enquête auprès des communes de moins de 3500 habitants pour comprendre leurs usages et leurs besoins. Ils ont choisi ces cibles car ces communes représentent 91% des collectivités. Paradoxalement ce sont celles qui sont le moins impliquées ou mises en avant des les programmes d'accompagnement.

Il ressort des réponses que la majorité des répondants dispose d'un parc informatique réduit, de moins de 5 postes. L'une des raisons est la faible part de budget allouée à l'équipement informatique. Le second constat est que ces mêmes collectivités n'ont pas de responsable informatique et externalisent la gestion de leur parc. Ils font souvent appel à un prestataire informatique local, en le faisant intervenir lorsqu'ils ont besoin. Pour eux, c'est un mode de fonctionnement simple et pratique mais qui présente des défauts.

Une de ses défauts inhérent est le manque de formation et de sensibilisation à ces sujets autour de la cybersécurité. Ils font confiance au prestataire car ils ne comprennent pas réellement les enjeux et leurs obligations. Il demeure qu'ils sont responsables de la sécurité de leur système d'information. Il arrive régulièrement qu'ils aient des usages risqués comme le partage de mots de passe ou le mélange personnel professionnel pour les élus.

Préconisations en matière de cybersécurité :

Les résultats de cette étude ont poussé Cybermalveillance à sortir un guide "Obligations et responsabilités des collectivités locales en matière de cybersécurité". C'est un document qui complète le guide "Sécurité numérique des collectivités territoriales" de l'ANSSI plus détaillé sur les réglementations applicables en la matière.

Ce guide rappelle de manière synthétique les différentes réglementations à prendre en compte avec les obligations liées. Il est fait mention entre autres de l'obligation de nommer un délégué à la protection des données(DPO) dans le cadre de la démarche de mise en conformité RGPD. Sur la partie plus technique, la nomination d'un responsable de la sécurité de la sécurité du système d'information(RSSI) permet d'avoir un expert pour piloter la politique de sécurité de la collectivité.

Ces deux postes ne sont pas présents dans toutes les collectivités pour différentes raisons. Pour pallier au manque de moyens, ces services peuvent être externalisés voire mutualisés pour un groupement de collectivités.

Le guide revient aussi sur les obligations liées au Référentiel général de sécurité et le Règlement eIdas. Ces deux textes vont s'appliquer en matière de certificats électronique de signature ainsi que pour la mise en place de téléservices. Les collectivités peuvent proposer de réaliser des démarches administratives en ligne par le biais d'un téléservice qui doit répondre à certains critères pour être valide, notamment par son homologation. De manière courante, les agents comme les élus utilisent des certificats de signature avec la dématérialisation des services publics. Des règles de sécurité supplémentaires s'appliquent aussi lorsque des données de santé sont concernées avec la notion d'hébergeur de données de santé certifiés. Pour comprendre ces textes, le DPO et le RSSI sont essentiels.

Conséquences d'une cyberattaque :

Pour mieux comprendre la nécessité de la cybersécurité, il faut avoir conscience des risques en cas de cyberattaque.

Le premier risque tient à l'image de la collectivité, pouvant fragiliser le lien de confiance. Le fait qu'un service soit indisponible ou que des données personnelles d'administrés soient publiées fait mauvaise presse auprès des administrés concernés.

Le second risque est financier, qu'il touche de manière directe la collectivité ou une structure tierce de manière indirecte. La collectivité devra payer pour la reconfiguration du système d'information après une cyberattaque, parfois cher selon l'étendue des dégâts. Par rebond des équipements publics peuvent être rendus indisponibles, avec un manque à gagner pour le gestionnaire.

Le dernier risque est le risque physique si le dysfonctionnement provoque des dommages aux personnes ou aux biens. La collectivité se doit d'assurer la sécurité des administrés.

Pour illustrer la partie financière, deux communes ont partagé récemment ce que leur a coûté la remise en service du parc informatique en plus des autres frais liés à la cyberattaque qu'ils ont subi.
L'attaque la plus récente est celle de six collectivités de la Communauté de communes coeur de de Maurienne Arvan(3CMA) en février 2022. Ils se sont vite remis de l'attaque car elle a été contenue rapidement sans faire trop de dégâts. Cela leur a coûté tout de même 300 000 € dont 135 000 € pour l'intervention d'une société labellisée par l'ANSSI. Le reste correspond à la prolongation d'un trimestre de la location du bâtiment qu'ils devaient quitter ainsi que d'autres frais. Ils ont déjà prévu un investissement pour la sécurisation du système avec une partir subventionnée par l'ANSSI.
L'attaque précédente a eu lieu en novembre 2020 dans la commune de Bondy. Ils en payent encore les conséquences aujourd'hui et prévoient un retour à la normale d'ici un an. Le problème majeur est que les deux serveurs redondants ont été cryptés et ils n'avaient pas de sauvegarde externe depuis 5 ans. Ils ont dû tout reconstruire de zéro en investissement environ 1,5 millions d'euros. En plus des conséquences financières, ils ont fait face à une crise sociale six mois après l'attaque à cause d'erreurs et de retard dans le versement des salaires. S'ils avaient eu une sauvegarde externe, ils auraient pu s'en remettre plus vite s'ils n'avaient pas dû remonter les bases de données de zéro.

Moyens de sensibilisation à la cybersécurité :

Cybermalveillance.gouv a déduit de l'enquête quatre préjugés des collectivités par rapport à la cybersécurité :
"Je n'ai pas le budget"
"Je n'ai pas le temps"
"Ce n'est pas ma priorité"
"Je n'y connais rien, je ne suis pas concerné"
Ils ont basé une campagne de sensibilisation à partir de ces quatre problématiques en s'inspirant de fables de La Fontaine. Ils ont produit des vidéos courtes détournant les fables ainsi que des visuels. Ils abordent le sujet d'une manière qui peut attirer plus de public par son côté décalé. Ce n'est pas la première fois qu'ils communiquent sur le sujet de manière ludique. Ils ont produit des contenus à destination des enfants comme des incollables. Ils publient régulièrement des informations et des guides selon les problématiques du moment.

Exemple de visuel inspiré du Lièvre et la Tortue :

Pour conclure, on constate que toutes les collectivités ne sont pas au même niveau de maturité sur le sujet de la cybersécurité. Trop souvent elles réagissent trop tard, après une attaque, et en payent le prix fort. C'est une problématique essentielle pour les collectivités quelque soit leur taille, avec des mesures adaptées. Ces collectivités ne sont pas seules pour y faire face, elles peuvent s'appuyer sur l'ANSSI par exemple pour les accompagner et les aider financièrement. Des structures de mutualisation peuvent aussi être une solution pour partager les coûts.

RÉFÉRENCES

Etude sur la vision de la cybersécurité par les communes de moins de 3500 habitants : :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/etude-cybersecurite-collectivites-moins-de-3500-habitants

Guide sur les obligations et les responsabilités des collectivités locales en matière de cybersécurité :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillance-gouv-fr-et-la-cnil-publient-un-guide-sur-les-obligations-et-les-responsabilites-des-collectivites-locales-en-matiere-de-cybersecurite

Guide de l'ANSSI sur la sécurité numérique des collectivités territoriales :

- https://www.ssi.gouv.fr/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/

Informations sur le référentiel général de sécurité :

- https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

Règlement eIdas :

- https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/
- https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=hr

Cyberattaque de Bondy :

- https://www.ouest-france.fr/ile-de-france/bondy-93140/seine-saint-denis-victime-d-une-cyberattaque-bondy-estime-les-dommages-a-1-5-million-d-euros-7856000
- https://www.leparisien.fr/seine-saint-denis-93/seine-saint-denis-la-cyberattaque-de-2020-a-coute-environ-15-million-deuros-a-la-mairie-de-bondy-11-07-2022-JRQAFP4ZRBHXVJNPRB2YC4JLIM.php
- https://www.lagazettedescommunes.com/743528/bondy-cyberattaque-en-novembre-greve-en-avril/

Cyberattaque de 3CMA :

- https://www.lagazettedescommunes.com/813552/cyberattaque-sur-une-communaute-de-communes-le-cout-de-la-riposte/?abo=1

Campagne de sensibilisation de cybermalveillance.gouv :

- https://creapills.com/fables-la-fontaine-cybersecurite-cybermalveillance-20220602
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/campagne-de-sensibilisation-les-freins-des-collectivites-en-matiere-de-cybersecurite

SUPPLEMENT JEUX

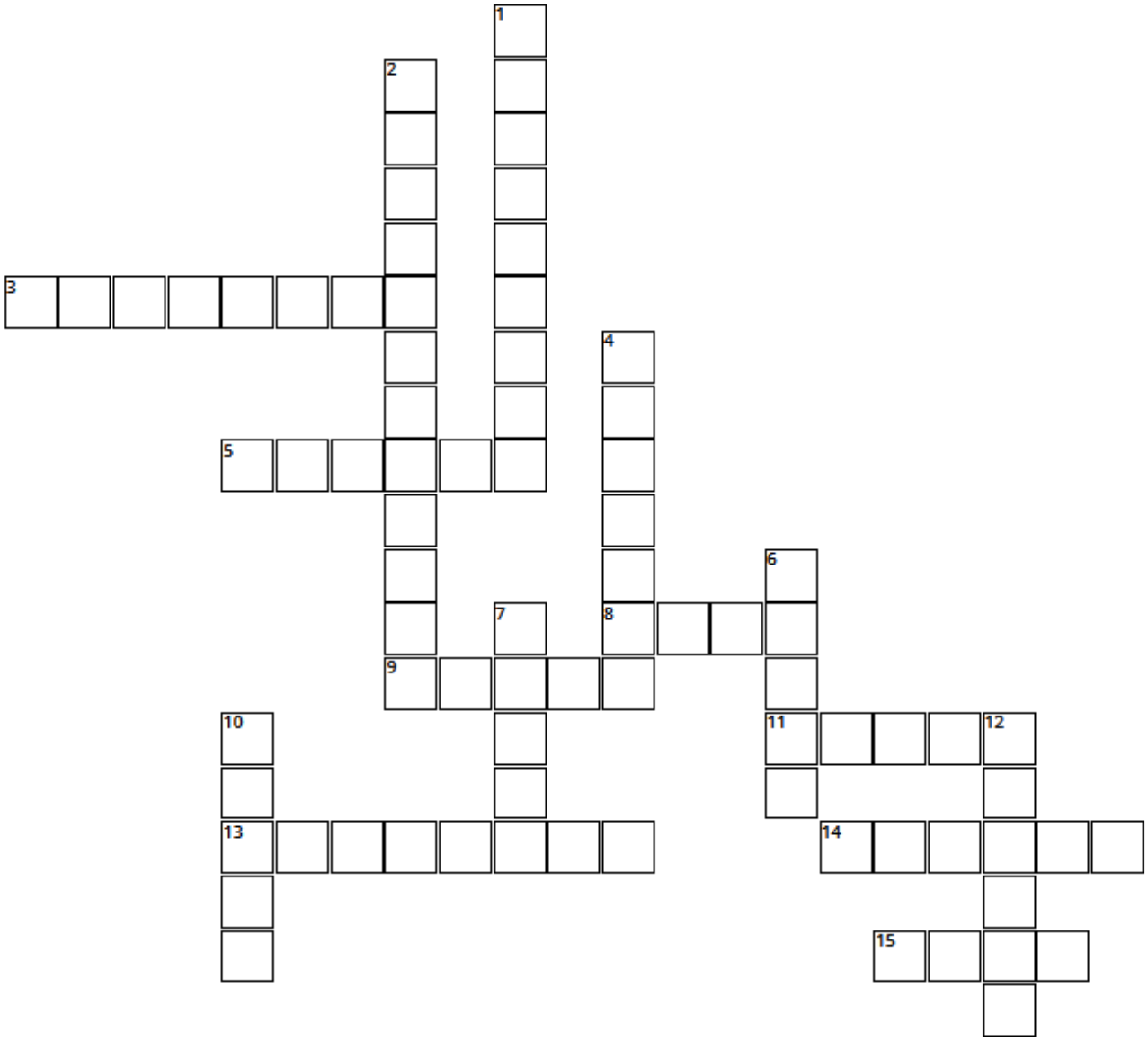
Voyons voir ce que vous avez retenu de votre lecture.
Tous les mots sont extraits des articles, à vous de retrouver lesquels !
Vous trouverez aussi la solution pour le mois de juin sur la page suivante

Horizontal

3. période entre 2 budgets
5. personnage du marvel cinematic universe
8. chanteuse surnomméela déesse de la pop
9. période studieuse autonome
11. rejoint par Emile en 1999
13. plan qui concrétise un projet professionnel
14. dans le rouge certains mois
15. botanique ou informatique

Vertical

1. suspensive pour l'achat d'un bien
2. autorité publique distincte de l'Etat
4. enchère pour les joueurs
6. qualifiés de faux lorsqu'ils sont mineurs
7. Le petit routard pour les voyageurs
10. histoire d'animaux en prose
12. star des séries policières américaines



SUPPLEMENT JEUX

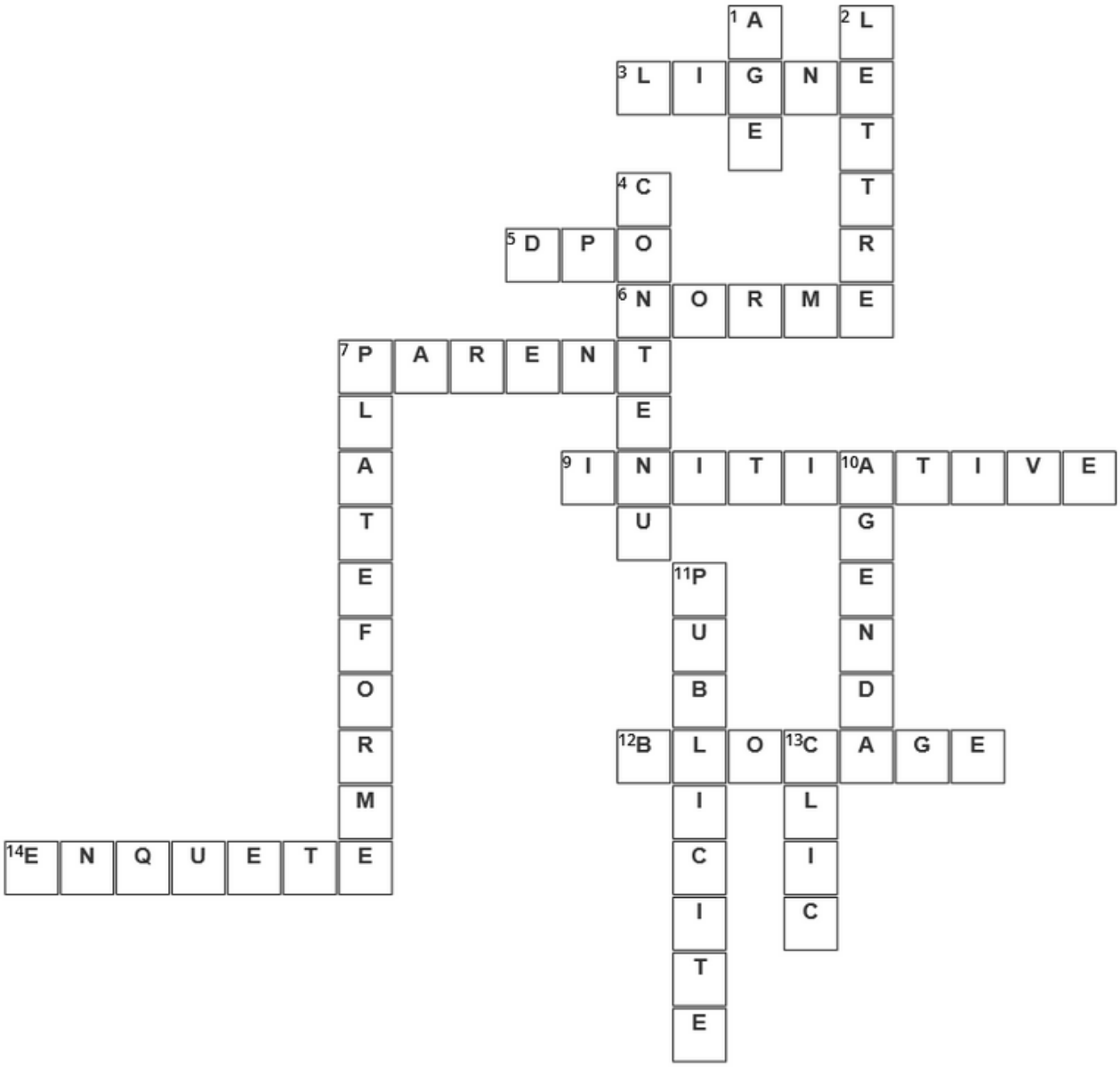
Solution pour la grille du mois de juin

Horizontal

3. plus facile à tracer avec une règle
5. désignation obligatoire pour les collectivités depuis mai 2018
6. Iso 27001 pour les systèmes des management de la sécurité de l'information
7. synonyme d'ascendant
9. ancien nom de syndicat pour le tourisme
12. possible réaction psychologique face à une situation nouvelle
14. préliminaire ou de flagrance

Vertical

1. ne se demande pas à une femme
2. chanson de renan luce sortie en 2006
4. à l'intérieur d'un contenant
7. type des premiers jeux mario
10. aide mémoire pour les rdv
11. objet de la réforme des actes administratifs de juillet 2022
13. bruit de la souris



SUPPLEMENT JEUX

Mots cachés sur le thème des vacances d'été
Les mots peuvent être horizontaux, verticaux ou en diagonale, bon courage !

3 lettres : mer
4 lettres : côte - vent
5 lettres : crème - glace - plage
6 lettres : sieste - soleil
7 lettres : chaleur - maillot - parasol - piscine
11 lettres : ventilateur
12 lettres : procrastiner

D	U	B	D	K	G	A	R	E	K	U	X	C	I
O	G	C	L	G	S	S	I	E	S	T	E	R	G
V	L	I	P	T	E	B	O	O	T	S	C	E	T
E	A	V	R	S	P	V	B	K	Y	I	H	M	S
N	C	E	O	B	I	K	W	Q	C	M	A	E	P
T	E	N	C	Z	S	K	I	P	O	A	L	A	A
I	A	T	R	N	C	F	P	T	C	I	E	A	R
L	C	W	A	D	I	H	L	J	K	L	U	L	A
A	Y	O	S	E	N	G	A	N	T	L	R	L	S
T	I	B	T	R	E	E	G	P	A	O	R	E	O
E	W	Y	I	E	D	Y	E	Q	I	T	E	R	L
U	Y	P	N	M	H	E	G	W	L	Y	E	G	Z
R	D	C	E	A	E	S	O	L	E	I	L	I	T
C	P	Q	R	Z	T	R	H	D	K	J	Y	E	J

SUPPLEMENT JEUX

4 images 1 mot

Saurez-vous retrouver le mot qui se cache derrière ces images ?

5 lettres : _____