Sujet élaboré par une cellule pédagogique nationale

CONCOURS INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2023

ÉPREUVE DE PROJET OU ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription, au sein de la spécialité dans laquelle il concourt.

Durée : 8 heures
Coefficient : 7

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 63 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes ingénieur territorial au sein du service d'administration des systèmes, réseaux et télécommunications du département d'Ingédep (2 000 agents).

Le système d'information de la collectivité est composé d'environ 300 serveurs et de 1800 postes de travail, répartis sur 75 sites différents.
Le système d'information des 40 collèges du département est composé d'environ 3 000 postes informatiques (pédagogiques et administratifs), 200 serveurs (entre 3 et 6 par collège), et de périphériques tels que des vidéoprojecteurs, des tableaux blancs interactifs (TBI), des imprimantes laser et des tablettes tactiles dans certains établissements.

Avec l'évolution massive des usages digitaux dans notre quotidien, la transition numérique est devenue un domaine prioritaire au sein des collectivités. Cette évolution exige le renforcement de la sécurité informatique face aux menaces et aux défis plus nombreux et plus complexes que jamais. De même, la migration vers le nuage (Cloud Computing) devient un véritable levier d'accélération de la transformation numérique des collectivités territoriales.

Dans ce contexte, Ingédep souhaite mener une réflexion de fond sur la sécurité de son infrastructure informatique en étudiant une ouverture progressive de certaines de ses activités vers le Cloud Computing.

Garant du bon fonctionnement et de la disponibilité des réseaux dont vous avez la responsabilité, il vous revient d'élaborer de nouvelles configurations pour optimiser la performance du réseau et la sécurité des systèmes d'information et anticiper le développement de nouveaux services aux usagers.

Question 1 (6 points)

Les collectivités territoriales sont les cibles privilégiées des attaques informatiques. Un cadre réglementaire leur impose la mise en place de différentes mesures destinées à sécuriser leurs systèmes d'information et protéger les données de leurs usagers.

Dans ce contexte, le directeur des systèmes d'information (DSI) vous demande :

a) de rédiger à son attention une note sur les nouveaux enjeux en matière de cybersécurité en détaillant les actions préventives à mettre en place pour garantir la sécurité informatique d'Ingédep ; (4 points)

b) de proposer une démarche visant à réaliser un audit du système d'information d'Ingédep. Vous décrirez pour cela les principales étapes, le rendu attendu et préciserez les différents acteurs à intégrer à cette démarche. (2 points)

Question 2 (5 points)

La majorité des menaces sont celles qui tentent de rentrer dans le réseau informatique depuis l'extérieur. Tout comme les antivirus, les firewalls sont en première ligne de défense pour protéger le réseau des collectivités.

a) Votre DSI vous demande de détailler l'intérêt technique et fonctionnel de migrer vers de nouvelles générations d'antivirus et de firewalls. (2 points)

b) Vous rédigerez, au travers d'un CCTP (principaux points), les principales fonctionnalités attendues de la future solution à mettre en place dans le cadre du renouvellement du firewall et de l'anti-virus. (3 points)

Question 3 (4 points)

Le Cloud Computing se positionne désormais comme une clé de transformation numérique qui s'opère actuellement dans les collectivités sur tout ou partie du système d'information.

Vous présenterez les bénéfices et les opportunités du Cloud Computing ainsi que ses faiblesses et points de vigilance.

Question 4 (5 points)

La collectivité d'Ingédep envisage de procéder à la migration de sa suite Office 2010 vers Office 365 en 2024. Pour cela, elle souhaite mener une première expérience en migrant une ou deux directions sur Office 365.

Votre DSI vous demande :

a) de proposer une démarche projet détaillant les principales étapes à conduire pour mener à bien cette migration ; (3 points)

b) d'élaborer le plan de communication à envisager à destination des différents acteurs concernés (élus, agents…). (2 points)

Liste des documents :

Document 1 : « Collectivités territoriales : quelle démarche adopter pour sécuriser durablement vos SI ? » - *amossys.fr* - 2 juillet 2018 - 2 pages

Document 2 : « Stratégie européenne pour la donnée : la CNIL et ses homologues se prononcent sur le Data Governance Act et le Data Act » - *CNIL* - 13 juillet 2022 - 5 pages

Document 3 : « RGPD : Assurer votre conformité en 4 étapes » - *CNIL* - 18 septembre 2019 - 5 pages

Document 4 : « Dans les collectivités, la transition numérique repose aussi sur la maîtrise de compétences numériques » - *Caisse des Dépôts* - 24 janvier 2022 - 5 pages

Document 5 : « Projet de Transformation Numérique ? Voici 5 étapes pour le réussir ! » - *visiativ.com* - 2 juin 2021 - 3 pages

Document 6 : « Qu'est-ce qu'un pare feu de nouvelle génération ? » - *archivesfactory.com* - 26 novembre 2020 - 2 pages

Document 7 : « Cloud : à quelles tendances doit-on s'attendre en 2022 ? » - *epsi.fr* - 15 avril 2022 - 2 pages

Document 8 : « Les grandes tendances de la cybersécurité en 2022 » - *sfrbusiness.fr* - 22 mars 2022 - 4 pages

Document 9 : « Qu'est ce qu'un Antivirus de Nouvelle Génération (NGAV) ? » - *crowdstrike.fr* - 24 mars 2022 - 5 pages

Document 10 : « L'offre Cloud Computing de l'UGAP : un nouveau marché pour accélérer la transformation digitale du service public » - *ugap.fr* - 24 janvier 2022 - 2 pages

Document 11 : « Doctrine Cloud au centre : quel impact pour le secteur public ? » - *wimi-teamwork.com* - 17 février 2022 - 3 pages

Document 12 : « Les enjeux de la transition numérique au sein des collectivités » - *nepsio.fr* - 26 avril 2022 - 3 pages

Document 13 : « SECURITE INFORMATIQUE : le Registre Général de Sécurité » - *sieeen.fr* - 25 janvier 2022 - 3 pages

Document 14 : « Pare-feu de nouvelle génération (NGFW) » - *fortinet.com* - consulté le 28 novembre 2022 - 3 pages

Document 15 : « Cybersécurité : l'Anssi veut renforcer son appui aux collectivités territoriales » - *Banque des territoires* - 17 octobre 2022 - 2 pages

Document 16 : « Cybersécurité : premier bilan pour l'accompagnement des collectivités » - *La Gazette des communes* - 13 juin 2022 - 2 pages

Document 17 : « Antivirus, EDR ou XDR : Quelle est la différence ? » - *cscience.ca* - 26 septembre 2022 - 2 pages

Document 18 : « Incendie d'OVH : une action collective lancée par sept entreprises » - *journaldunet.com* - 15 novembre 2021 - 6 pages

Dans le cadre de sa politique environnementale, la cellule pédagogique nationale privilégie des impressions en noir et blanc. Les détails non perceptibles du fait de ce choix reprographique ne sont pas nécessaires à la compréhension du sujet, et n'empêchent pas son traitement.

DOCUMENT 1

Collectivités territoriales : quelle démarche adopter pour sécuriser durablement vos SI ?

amossys.fr - Expertise et innovation en cybersécurité - le 02/07/2018

A l'heure où la cybersécurité fait quotidiennement les titres de l'actualité, les collectivités territoriales, au même titre que le secteur privé, représentent une cible de choix pour les pirates informatiques. Quelle démarche doivent-elles initier pour se protéger et sécuriser durablement leurs systèmes d'information ? Le point avec Jérôme LEBEGUE, responsable des activités Audit & Conseil chez AMOSSYS.

Vous êtes responsable des activités Audit & Conseil chez Amossys. Quelles sont les problématiques de cybersécurité pour lesquelles vos clients du secteur public vous sollicitent le plus ?

Les sollicitations tournent actuellement autour de trois principales thématiques :

- **Le réglementaire** ; que l'on soit sur le RGPD qui concerne tout le monde ou sur des problématiques d'homologation de systèmes pour les Organismes d'Importance Vitale (OIV).

- **Les audits techniques des plateformes exposées.** De plus en plus d'acteurs prennent conscience de l'impact en termes d'image mais aussi en termes juridique si le service exploite des données personnelles notamment.

- **Les audits internes** ; parfois après un incident parfois après la nomination d'un nouveau RSSI qui souhaite avoir un état des lieux de ses systèmes.

Globalement, on constate une prise de conscience de plus en plus forte sur le fait que la cybersécurité est un METIER à part entière. Les organisations font de moins en moins une confiance aveugle à leurs fournisseurs sur les aspects cyber.

Quelle démarche leur conseillez-vous d'adopter pour se prémunir des risques spécifiques auxquels ils s'exposent ?

Anticiper ! Plus la sécurité sera prise en compte tôt, moins elle coûtera : c'est aussi simple que cela.

De quelle manière Amossys peut-elle accompagner les acteurs publics ?

De par son expertise et son ancienneté dans le domaine, AMOSSYS est en capacité d'intervenir sur un large panel d'activités. Nous pouvons par exemple apporter notre expertise sous forme de conseil dans le cadre d'une organisation SSI qui se met en place ou lors d'une refonte.

Nous pouvons également accompagner les décideurs dans leurs problématiques cybersécurité sur les choix et les arbitrages à mener. Dans le cadre de projets plus globaux, nous pouvons intervenir à chaque étape du cycle, depuis la conception du produit jusqu'à la recette sécurité.

Enfin, nous réalisons des prestations de sensibilisation et de formation des équipes (architectes, administrateurs, développeurs) afin qu'ils soient armés pour faire face au risque cyber.

Pouvez-vous illustrer par quelques exemples ?

AMOSSYS adapte ses prestations d'accompagnement à la structure concernée. Nous sommes par exemple intervenus au sein de Communautés de Communes dans le cadre d'un premier état des lieux de sécurité (en incluant la thématique RGPD).

De la même façon, le cadre réglementaire renforcé pour les OIV avec la Loi de Programmation Militaire (LPM) nous a amené à renforcer nos interventions auprès de ces clients, avec des niveaux de maturités très variables. En tant que Prestataire d'Audit de la Sécurité des Systèmes d'Information AOSSYS est un acteur de choix pour ces thématiques et nous intervenons autant sur les phases d'accompagnement en amont, d'assistance à homologation que dans les phases d'audit de sécurité.

DOCUMENT 2

Stratégie européenne pour la donnée : la CNIL et ses homologues se prononcent sur le Data Governance Act et le Data Act

CNIL le 13 juillet 2022

Le 5 mai 2022, le Comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données (EDPS) ont adopté un avis sur la proposition de règlement européen sur les données (*Data Act*). Cet avis, qui succède à celui de mars 2021 sur la gouvernance des données (*DGA*), marque une étape supplémentaire dans la construction d'une économie européenne de la donnée respectueuse des libertés et droits fondamentaux.

Data Governance Act, Data Act : de quoi s'agit-il ?

Le *Data Governance Act* et le *Data Act* s'inscrivent dans le cadre de la stratégie européenne pour les données, présentée par la Commission européenne en février 2020. Cette stratégie vise à développer un marché unique de la donnée en soutenant l'accès, le partage et la réutilisation responsables, dans le respect des valeurs de l'Union européenne et notamment la protection des données personnelles.

Elle s'inscrit dans le contexte plus large du plan d'action de la Commission européenne visant à assurer la souveraineté numérique de l'Europe à l'horizon 2030, et est complémentaire de la stratégie européenne en matière d'intelligence artificielle.

Le règlement sur la gouvernance des données (*Data Governance Act*)

Première brique de la série de mesures annoncées dans le cadre de la stratégie européenne des données, le *Data Governance Act* a été adopté en mai 2022, et sera applicable en septembre 2023. Il vise à favoriser le partage des données personnelles

et non personnelles en mettant en place des structures d'intermédiation. Ce règlement comporte :

- un encadrement ainsi qu'une assistance technique et juridique facilitant **la réutilisation de certaines catégories de données protégées du secteur public** (informations commerciales confidentielles, propriété intellectuelle, données personnelles) ;
- **une certification obligatoire pour les fournisseurs de services d'**intermédiation de données ;
- **une certification facultative pour les organismes pratiquant l'**altruisme en matière de données.

Le règlement sur les données (*Data Act*)

La proposition législative de la Commission européenne, présentée le 23 février 2022, a pour objectif **d'assurer une meilleure répartition de la valeur issue de l'utilisation des données personnelles et non personnelles entre les acteurs de l'économie de la donnée,** notamment liées à l'utilisation des objets connectés et au développement de l'Internet des objets.

À ce titre, la proposition de *Data Act* a pour objectifs de :

- **faciliter le partage entre entreprises (B2B) et avec le consommateur (B2C) des données**, en fixant notamment une obligation de rendre accessibles les données générées par l'utilisation des objets connectés et services connexes, en contrepartie d'une compensation juste et équitable ;
- **permettre l'utilisation des données détenues par les entreprises et, sous réserve de justifier d'un besoin exceptionnel**, **par les organismes publics** des États membres et les institutions, agences ou organes de l'Union ;
- **faciliter le changement de fournisseur de services de traitement de données (*cloud* et *edge computing)*** par l'encadrement des relations contractuelles entre les fournisseurs de services et les consommateurs, et notamment par la suppression progressive des frais liés au changement pour le consommateur ;
- prévoir l'élaboration **de normes d'interopérabilité** pour les données et leurs réutilisations entre les secteurs ;
- mettre en place des **garanties contre les accès illicites de gouvernements de pays tiers** aux données non-personnelles contenues dans le cloud.

Les avis de la CNIL et de ses homologues

Les enjeux liés à l'articulation de ce nouveau cadre législatif sur les données avec le règlement général sur la protection des données personnelles (RGPD) ont conduit la

Commission européenne à solliciter l'expertise de la CNIL et de ses homologues. Le *Data Governance Act* et le *Data Act* nécessitent, sous des angles différents, deux éléments clés pour garantir leur bonne articulation avec le RGPD :

- la **cohérence** de ces futures dispositions avec les droits et obligations du RGPD ; et
- une **gouvernance intelligente gravitant autour des autorités de protection des données** afin d'assurer l'application efficace et effective des différents cadres juridiques et d'assurer leur lisibilité pour les citoyens et acteurs économiques concernés.

La nécessité de veiller à la cohérence avec le RGPD

Des objectifs légitimes et l'amélioration de certains droits et protections

Les autorités de protection des données et le Contrôleur européen reconnaissent l'objectif légitime du *DGA* de favoriser la disponibilité des données par la mise en place de structures d'intermédiation de données et par le renforcement des mécanismes de partage de données dans l'ensemble de l'Union. De même, l'objectif du *Data Act* de libérer le potentiel des données afin de développer des connaissances précieuses pour des secteurs tels que la science, la santé ou l'action climatique est accueilli favorablement par les autorités de protection des données et le Contrôleur européen.

Le *Data Act* pourra par ailleurs permettre un droit plus effectif à la portabilité des données en vue de faciliter l'innovation et de promouvoir la concurrence, et de permettre aux consommateurs de contrôler de manière significative la manière dont leurs données générées par l'utilisation des objets connectés sont utilisées.

Enfin, l'encadrement des demandes d'accès par des autorités étrangères et des transferts de données non-personnelles par ces deux règlements fera converger les modèles de protection des données personnelles et non personnelles.

Des garanties nécessaires pour préserver les droits des personnes

Dans le même temps, la protection des données personnelles est essentielle et fait partie intégrante de la confiance dans le développement de l'économie numérique. Le Comité européen de la protection des données et le Contrôleur européen de la protection des données ont appelé les co-législateurs (Parlement européen et Conseil de l'UE) à veiller à ce que le *DGA* et le *Data Act* ne portent pas atteinte à la protection des données personnelles. Les co-législateurs ont tenu compte de cette recommandation pour le *DGA* en spécifiant que le RGPD prévaudrait en cas de conflit avec le *DGA*.

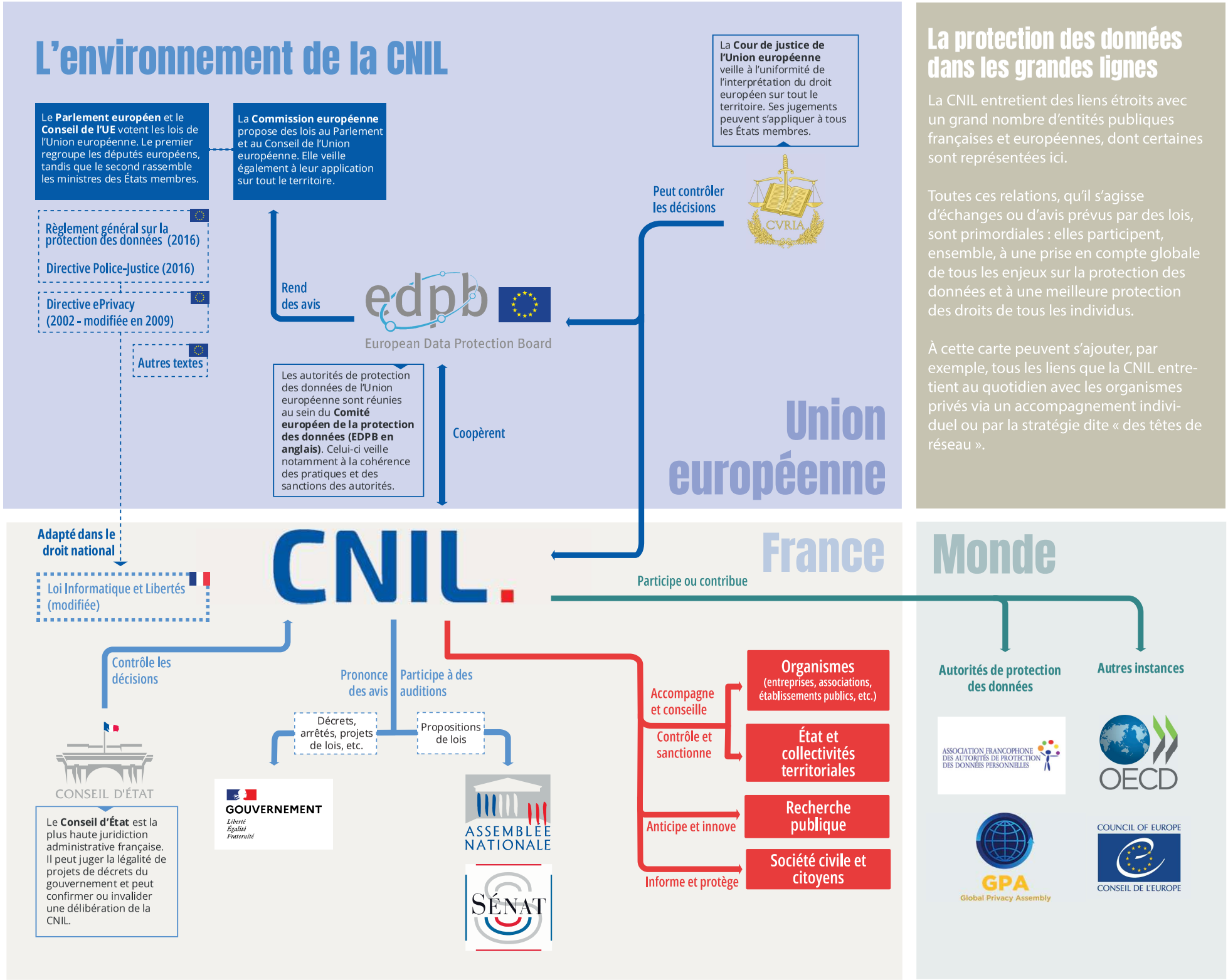
En ce qui concerne les droits d'accès, d'utilisation et de partage des données prévus par le *Data Act*, la CNIL et ses homologues demandent aux co-législateurs de mettre en place des garanties additionnelles pour les personnes concernées. Ils doivent également veiller à la légalité, la nécessité et la proportionnalité de l'obligation de mettre les données à la disposition des organismes du secteur public et des institutions de l'UE en raison d'un besoin exceptionnel, et définir plus strictement les hypothèses d'« urgence publique » ou de « besoin exceptionnel ».

La nécessité d'assurer une gouvernance intelligente

La CNIL et ses homologues alertent également sur le fait que la non-désignation des autorités chargées de la protection des données pour la supervision du *DGA* pourraient entraîner une réelle **complexité pour les acteurs numériques et les personnes concernées, et nuire à la cohérence de la surveillance de l'application du RGPD**. Les co-législateurs ont toutefois indiqué que les autorités de protection des données pouvaient être considérées comme des autorités compétentes pour le *DGA*.

De même, la désignation des autorités de protection des données comme autorités compétentes pour le *Data Act* permettra d'éviter les incohérences avec le droit fondamental à la protection des données personnelles et d'assurer un guichet unique aux acteurs de la donnée. Les co-législateurs devraient donc **désigner les autorités de protection des données comme autorités coordinatrices pour l'application de l'ensemble du *Data Act*.** En effet, les autorités de protection des données ont une **expertise juridique et technique** dans la supervision des traitements de données personnelles, et l'accompagnement des acteurs et modèles d'affaires innovants.

L'environnement de la CNIL



La protection des données dans les grandes lignes

La CNIL entretient des liens étroits avec un grand nombre d'entités publiques françaises et européennes, dont certaines sont représentées ici.

Toutes ces relations, qu'il s'agisse d'échanges ou d'avis prévus par des lois, sont primordiales : elles participent, ensemble, à une prise en compte globale de tous les enjeux sur la protection des données et à une meilleure protection des droits de tous les individus.

À cette carte peuvent s'ajouter, par exemple, tous les liens que la CNIL entretient au quotidien avec les organismes privés via un accompagnement individuel ou par la stratégie dite « des têtes de réseau ».

DOCUMENT 3

RGPD : Assurer votre conformité en 4 étapes

CNIL le 18 septembre 2019

La démarche de conformité RGPD ne doit pas être perçue que comme une contrainte technique ou juridique. C'est avant tout l'occasion de faire le point sur l'utilisation des services numériques dans la collectivité et de s'assurer que la protection des données personnelles a bien été prise en compte. La mise en conformité au RGPD passe par plusieurs étapes successives et certaines de ces actions doivent perdurer dans le temps pour être efficaces (formation, évolution des procédures, etc.). Il s'agit d'une démarche active et en continu.

1. Recenser les traitements

Le RGPD impose au responsable de traitement de tenir un registre listant les traitements de données. Il vous permet d'avoir une vision claire et globale des activités de la collectivité qui nécessitent la collecte et le traitement de données personnelles.

La tenue du registre est l'occasion de sensibiliser les services aux enjeux de la protection des données. Dans les faits, ce registre est souvent tenu par le DPO.

Dans votre registre, créez une fiche par activité recensée, en précisant :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- le ou les objectifs poursuivis par chaque traitement (finalité(s) du traitement ex : tenue de l'état civil) ;
- les catégories de personnes concernées et de données utilisées (ex : nom, nationalité, adresse, etc.) ;
- qui a accès aux données (personnes habilitées – ex : service RH pour la paie) et à qui elles seront communiquées (les destinataires - ex : les services des impôts) ;
- les durées de conservation de ces données (durée d'utilité et durée de conservation en archive) ;
- les mesures de sécurité envisagées (ex : politique des mots de passe, etc.) ;
- le cas échéant, les transferts de données à caractère personnel en dehors de l'UE ou à une organisation internationale.

Pour avoir un registre exhaustif et à jour, il est nécessaire d'être en contact régulier avec toutes les personnes de la collectivité susceptibles de traiter des données personnelles.

2. Faites le tri dans vos données

Chaque fiche du registre vous permet de vérifier :

- **que les données traitées sont bien pertinentes et nécessaires à l'objectif poursuivi (principes de pertinence et de minimisation).**

Exemple de pertinence : pour l'inscription à l'école élémentaire, il est légitime de demander un livret de famille, un justificatif de domicile et un document attestant que l'enfant a reçu les vaccinations obligatoires pour son âge.
Lors d'une inscription scolaire, il n'est en revanche pas pertinent de demander le numéro de sécurité sociale du ou des représentants légaux ou encore la copie de leur carte Vitale. Pour la gestion de la cantine scolaire, il suffit d'enregistrer uniquement les informations relatives au régime alimentaire et aux aliments à proscrire pour un élève plutôt que d'inscrire son état de santé (ex. : « diabétique ») ou de mentionner sa religion.

- **la nature des données traitées afin d'adopter des mesures de sécurité adaptées aux risques spécifiques associés aux données.**

Exemple de mesure de sécurité : les établissements scolaires et périscolaires sont amenés à collecter des données relatives à la santé des mineurs qu'ils accueillent dans le cadre des projets d'accueil individualisé (PAI). Dans la mesure où ces informations sont sensibles, elles doivent faire l'objet de mesures de protection particulières (rangement sécurisé, etc.).

- **que seuls les agents habilités ont accès aux données dont ils ont besoin.**

Exemple de destinataire : dans le cadre des demandes d'actes d'état civil, l'accès aux informations nécessaires à l'instruction de ces demandes doit être limité aux seuls agents chargés de cette activité.

- **que les données ne sont pas conservées au-delà de ce qui est nécessaire en fixant précisément la durée de conservation et d'archivage des données (principe de durée limitée de conservation des données).**

Exemple de durée de conservation : dans le cadre d'un fichier de prévention de la délinquance mis en oeuvre par une mairie, les données sur une personne peuvent être conservées pendant le temps du suivi. Les données peuvent ensuite être conservées en archive durant 3 ans après la fin du suivi. En tout état de cause, dans la mesure où dans le cadre des programmes de prévention de la délinquance, les personnes concernées ne peuvent être suivies que jusqu'à 25 ans, aucune donnée ne doit être conservée au-delà de cette limite d'âge.

3. Respecter les droits des administrés

Le nombre toujours croissant de plaintes reçues par la CNIL témoigne de la sensibilité accrue des personnes concernant la protection de leurs données personnelles. En 2018, près de 74 % des plaintes reçues concernent l'exercice pratique des droits : absence de réponse de la part des organismes ou refus non motivé, absence de procédure en ligne pour exercer ses droits, etc.

Informez les personnes dont vous traitez les données

Chaque fois que des données personnelles sont recueillies, que ce soit sur un formulaire, par l'intermédiaire d'un téléservice ou par oral, vous devez informer en toute transparence les personnes concernées des conditions d'utilisation de leurs données et de leurs droits, en particulier :

- vos coordonnées (le nom et les coordonnées du responsable du traitement) ;
- pourquoi vous collectez ces données (l'objectif de la collecte des données,
- par exemple pour gérer l'état civil) ;
- ce qui vous autorise à traiter ces données (l'exécution d'une mission de service public,
- le consentement de la personne concernée, etc.) ;
- qui a accès aux données (les services internes compétents, un prestataire, etc.) ;
- combien de temps vous conservez les données (la durée de conservation) ;
- comment les personnes peuvent exercer leurs droits (via leur espace personnel
- ou par un message adressé au DPO) ;
- si vous transférez les données hors de l'Union européenne (notamment par le biais
- d'un sous-traitant, le pays et l'encadrement juridique qui maintient le niveau
- de protection des données doivent être précisés).

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez, par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité/page vie privée sur votre site web.

Organisez et facilitez l'exercice des droits des administrés et des agents

Les personnes (agents, administrés, prestataires, etc.) ont des droits sur leurs données.
Vous devez permettre aux personnes d'exercer effectivement et le plus simplement possible leurs droits :

- **droit d'accès :** la personne accède à toutes les informations détenues sur elle ;

- **droit de rectification :** la personne modifie des informations détenues sur elle ;
- **droit d'opposition :** la personne refuse l'utilisation des informations détenues sur elle ;
- **droit d'effacement :** la personne demande la suppression des informations détenues sur elle ;
- **droit à la portabilité :** la personne récupère dans un format ouvert et lisible par machine les informations détenues sur elle ;
- **droit à la limitation :** la personne demande à « geler » l'utilisation des informations détenues sur elle.

Ces droits comprennent chacun des exceptions et des limitations spécifiques, en fonction de la base légale du traitement ou de son contexte. Par exemple, le droit d'opposition ne s'applique pas aux traitements dont la base légale est le respect d'une obligation légale (fichiers d'état civil ou fiscal).

Bonne pratique

Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez aux administrés la possibilité d'exercer leurs droits à partir de leur compte.
Mettez en place, par l'intermédiaire du DPO, un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois maximum).

4. Sécurisez les données

Vous devez mettre en place des mesures techniques et organisationnelles pour garantir la sécurité des données. En fonction de leur sensibilité, des mesures spécifiques sont nécessaires en cohérence avec les risques pour les droits et libertés des personnes concernées (ex : usurpation d'identité).
Trois types de risques sont ainsi à considérer : l'accès illégitime à des données, leur modification non désirée et leur disparition. Ces risques ne sont pas théoriques. Tous les jours, la CNIL reçoit des notifications de violation de données qui témoignent des faiblesses de la sécurisation de nombreux systèmes d'information. Ces incidents peuvent avoir des conséquences très préjudiciables pour les personnes dont les données sont concernées et des répercussions réputationnelles très importantes pour les organismes.

Bonne pratique

Les agents disposent d'un identifiant propre avec un mot de passe personnel, complexe, et régulièrement mis à jour. Leurs accès aux fichiers sont définis en fonction de leurs besoins réels en lien avec l'exercice de leur mission et leurs comptes

informatiques sont clos à la fin de leur contrat. Les armoires sont fermées à clé. Les mots de passe sont changés régulièrement et ils sont suffisamment complexes.

Voici quelques vérifications que vous pouvez déjà effectuer

- les accès aux locaux sont-ils sécurisés ?
- les armoires et coffre-fort sont-ils fermés à clés systématiquement ?
- les comptes utilisateurs sont-ils protégés par des mots de passe d'une complexité suffisante ? Sont-ils clos à la fin des contrats des agents ?
- des profils distincts sont-ils prévus selon les besoins des utilisateurs pour accéder aux données ?
- les postes de travail sont-ils sécurisés (ex : verrouillage automatique de session, antivirus et logiciels à jour) ?
- le personnel est-il sensibilisé à la protection de la vie privée ?
- Une charte informatique est-elle signée ?
- des mobiles multifonctions (smartphone), ordinateurs portables ou clé USB sont-ils utilisés ? Leur usage est-il encadré ?
- des procédures de sauvegardes régulières et de récupération des données en cas d'incident sont-elles mises en place ?

Que faire en cas de violation de données ?

Des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées (courriels transmis à des mauvais destinataires, équipement perdu ou volé, publication involontaire de données sur internet, etc.) ? Cet incident constitue une « violation de données ».
Si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées, vous devez la signaler à la CNIL dans les 72 heures. Cette notification s'effectue en ligne sur le site web de la CNIL.
Si ces risques sont élevés pour ces personnes, vous devrez les en informer.

DOCUMENT 4

Dans les collectivités, la transition numérique repose aussi sur la maîtrise de compétences numériques

Caisse de dépôts le 24 janvier 2022

Les évolutions de l'action publique, les attentes fortes des usagers (dématérialisation, accueil et accompagnement du public en présentiel et à distance, open data etc.) renforcées pendant la crise sanitaire, ont incité l'Etat à mobiliser 1,7 milliards d'euros pour soutenir la transformation numérique de l'Etat et des collectivités territoriales dans le cadre du plan de relance.

L'enjeu des compétences numériques des agents territoriaux a été mesuré : 25% d'entre eux n'ont pas une pratique autonome des compétences numériques basiques, telles que l'usage de courriels, d'outils collaboratifs, des fonctionnalités basiques de gestion des fichiers, tandis que leurs métiers évoluent par nature vers davantage de médiation, d'accompagnement des usagers, et l'utilisation d'outils numériques et utilisant des données

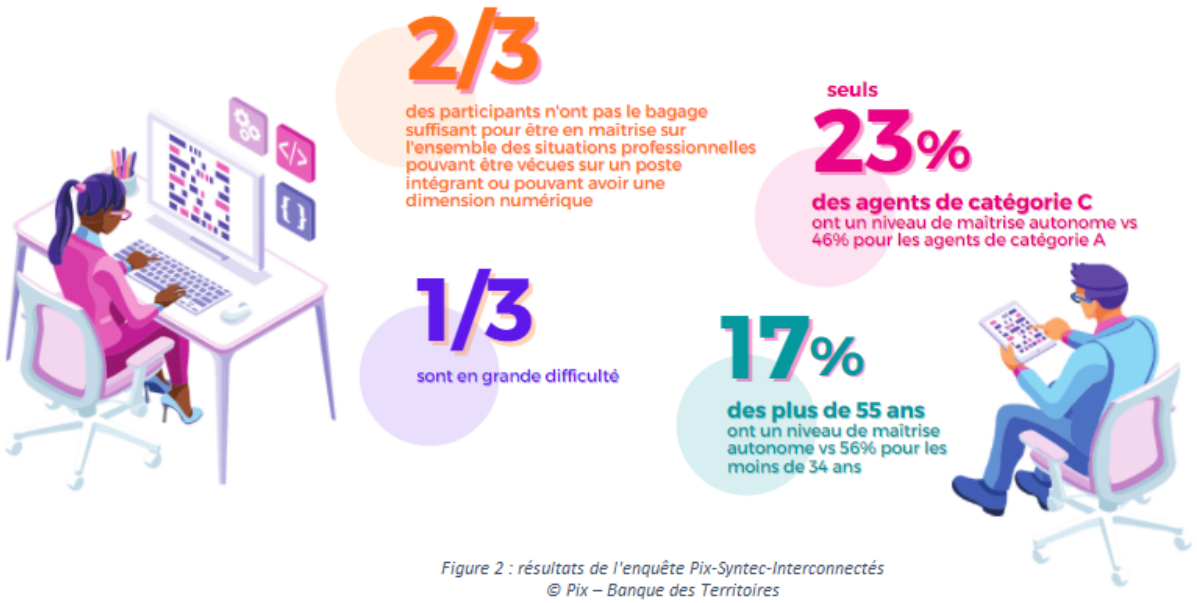


Figure 2 : résultats de l'enquête Pix-Syntec-Interconnectés
© Pix – Banque des Territoires

Ces constats révèlent une marge de progrès encore importante, mais dans les communes, les conseils départementaux et régionaux, les initiatives dédiées à l'autonomie numérique des agents (évaluation, formation, médiation) sont en plein essor.

L’impact du numérique sur les métiers des agents, une préoccupation récente pour les collectivités et qui s’accélère avec le développement du télétravail et de la dématérialisation.

Si l’informatisation du secteur public local a commencé il y plus de 20 ans, la prise de conscience de son impact sur les compétences à maîtriser est beaucoup plus récente.

Le CNFPT a mené une étude relative à l’impact du numérique sur les métiers de la fonction publique territoriale sur plus d’un an auprès de 300 acteurs dont 159 collectivités. Les travaux ont mis en évidence un besoin urgent de développer l’acquisition de compétences socles liées aux usages du numérique.

Toutefois, la numérisation des métiers des collectivités implique également des montées en compétences plus spécifiques. 42 métiers vont nécessiter à court terme une montée en compétences : communication, finances, planification mais aussi les métiers d’accueil et de médiation (services sociaux, voirie, culture, agents d’accueil…) sont particulièrement exposés à la dématérialisation des outils et des procédures.

Pour le CNFPT, les collectivités sont entrées dans "une nouvelle phase de la transition numérique" liés :

- à l’intégration des nouvelles technologies,
- aux obligations réglementaires de dématérialisation, open data…,
- au niveau des pratiques numériques des habitants,
- aux nouveaux modes d’organisation et de travail induits ou favorisés par le numérique comme le télétravail, recours au distanciel, travail en réseau et en mode collaboratif.

L’ensemble des 241 métiers territoriaux sont impactés "dès maintenant" par la transition numérique selon leur analyse.

Passer d’une logique « outil » à une logique « compétences » dans les démarches d’accompagnement

La logique de formations bureautique, outil par outil, a montré ses limites face à la diversité d’outils à manipuler et leur constante évolution. L’approche alternative consiste à cibler l’acquisition compétences permettant d’être autonome dans des situations quotidiennes ou nouvelles, de manière à pouvoir s’adapter aux changements ou à l’arrivée de nouveaux outils, et chercher des réponses par soi-même.

L’Union Européenne a développé un cadre de référence de compétences numériques regroupées dans 5 grands domaines. Ce cadre de référence est un point de départ. Chaque catégorie se décline ensuite en compétences simples (saisir du texte dans un logiciel d’édition) jusqu’à des compétences plus complexes (coder une page web en html).

Dans une démarche d’accompagnement, tout l’enjeu est donc d’identifier celles qui sont pertinentes pour un métier donné, et le niveau de maîtrise attendu.

Un socle de compétences numériques commun à tous les agents, et des compétences spécifiques complémentaires selon les métiers

La Banque des Territoires et son partenaire Pix ont mené des travaux pour identifier les compétences les plus importantes pour les métiers de la fonction publique territoriale. Pix est une startup d’Etat qui s’appuie sur le cadre de référence européen pour proposer un service en ligne permettant de mesurer, développer et certifier ses compétences numériques aujourd’hui utilisé par plus de 7 millions d’utilisateurs.

A ce jour, plusieurs dizaines de collectivité ont déjà mis en œuvre des stratégies d’accompagnement pour :

- Cartographier les compétences numériques maîtrisées ;
- Mettre en place d’un plan de formation adapté aux besoins des agents ;
- Suivre dans la durée de l’acquisition des compétences.

Ces retours d’expériences ont fait apparaître l'intérêt de construire un référentiel de compétences dédié aux collectivités territoriales. Les travaux de la Banque des Territoires et Pix ont permis d’identifier deux groupes de compétences :

- un socle de compétences pour l’ensemble des agents (figure 2)
- et des référentiels orientés métiers (figure 3).

Figure 2 : socle de compétences numériques à maîtriser par tous les agents
© Pix – Banque des Territoires

Figure 2 : socle de compétences numériques à maîtriser par tous les agents
© Pix – Banque des Territoires

Des parcours d'évaluation de ces compétences ont été conçus dans le cadre du partenariat de la Banque des Territoires et Pix. Ils seront expérimentés par une trentaine de collectivités de février à avril 2022. Suite à l'expérimentation, ces parcours seront intégrés à l'offre de Pix dédiée aux collectivités.

Conclusion : Vers une approche intégrée de la transition numérique

L'évolution vers la numérisation de plus en plus de procédures, de services aux usagers et des outils métiers est inéluctable et rend la prise en compte des compétences numériques incontournables.

Toutefois, toute démarche d'accompagnement des compétences doit également tenir compte de l'environnement numérique dans laquelle elle se situe :

- **La connectivité du territoire**, notamment dans les zones rurales et en Outre-Mer, pour lesquels la Banque des Territoires est engagée à offrir des solutions de financement aux collectivités et acteurs privés.
- **La disponibilité des données à jour et de services performants** : du pilotage stratégique du territoires aux interventions des services techniques, la capacité à accéder à des données à jour et à des outils permettant de les exploiter devient un enjeu de souveraineté pour les collectivités.
- **L'accès à du matériel adapté** : avec la numérisation des activités professionnelles, le besoin de matériel adapté (webcam, micro, tablette, smartphone,…) est exprimé par les agents et particulièrement pour les professionnels de la médiation numérique.

DOCUMENT 5

Projet de Transformation Numérique ? Voici 5 étapes pour le réussir !

visiativ

le 2 juin 2021

La transformation digitale des entreprises n'est plus un sujet nouveau. Cela dit, le contexte pandémique, l'a largement remis sur le devant de la scène. En effet, dans une période de « digital forcé », nombreuses sont les organisations qui se sont rendues comptes, qu'elles n'étaient pas encore au point en la matière !

Les **5 étapes clés pour réussir son projet de transformation numérique**. Votre temps est précieux, nous le savons ! Nous vous proposons donc aujourd'hui un condensé pour en retenir l'essentiel.

1	2	3	4	5
LE DIAGNOSTIC	L'ANALYSE DES BESOINS	LA GESTION DES DONNEES	L'HUMAIN ET LA FORMATION	LA MESURE DES RESULTATS

LA PREMIERE ETAPE DU PROJET DE TRANSFORMATION NUMERIQUE : LE DIAGNOSTIC

Il s'agit d'une étape incontournable. Dans tout projet, on insiste sur l'importance de fixer des objectifs. Effectivement, il est indispensable de définir où on veut aller. Mais pour cela, il est tout aussi important de savoir d'où l'on part !

➜ Évaluer son niveau de digitalisation

Le diagnostic va donc permettre à l'entreprise ou l'organisation de définir où elle se positionne dans le processus de digitalisation sur une échelle allant de 0 à 10, c'est-à-dire de « pas du tout digitalisée » à « totalement digitalisée ».

➜ Éléments évalués

En termes concrets, le diagnostic va consister à formaliser le niveau de digitalisation de l'entreprise, notamment en listant ce qui est déjà digitalisé, ce qui est en cours de digitalisation, ce qui ne l'est pas et pourrait l'être.

Ceci va permettre d'avoir une vision claire sur le niveau de digitalisation et d'identifier les actions prioritaires à mener pour démarrer ou poursuivre le processus de transformation numérique.

Vous l'aurez compris, cette étape est donc cruciale dans votre projet. Pour vous y aider, Visiativ a conçu un outil de diagnostic en ligne, constituant une bonne base de départ pour vous lancer.

DEUXIEME ETAPE : ANALYSER LES BESOINS

Les éléments et processus prioritaires une fois identifiés, il convient de les hiérarchiser et d'identifier les besoins précis. Ceci orientera le choix des solutions à mettre en place.

➜ Établir sa feuille de route numérique

Définir des priorités et se fixer des échelons dans le temps sont les clés de la réussite de votre projet de transformation numérique. Établir une feuille de route est donc essentiel, afin d'y voir clair et de ne pas se perdre en chemin !

➜ Des critères propres à l'entreprise

La priorisation des périmètres à adresser se fait en fonction de critères qui sont propres à l'organisation. Enjeux stratégiques, budgets, ressources … sont autant d'éléments qui orienteront la construction de votre feuille de route.

ÉTAPE TROIS : ANTICIPER SUR LA GESTION DES DONNEES

Digitaliser c'est, de fait, générer de la data. Il faut donc s'interroger sur la façon avec laquelle seront gérées ces données. Cette réflexion devra prendre en compte au moins quatre axes :

➜ La sécurité et l'accès aux données

Vous devez être en mesure de maîtriser l'accès aux données. Autrement dit, qui peut accéder à quoi, aussi bien en interne qu'en externe.

Bien entendu, il faudra vous protéger contre les attaques malveillantes.

➜ Le mode de stockage

Bien souvent plusieurs modes de stockages coexistent. Il est important de bien les maîtriser afin d'exploiter au maximum vos données.

➜ Le partage d'information

Posséder des données c'est bien, pouvoir les partager à bon escient avec les bonnes personnes c'est mieux ! Il est donc essentiel de permettre ses échanges entre collaborateurs ou avec un écosystème extérieur de façon maîtrisée et sécurisée.

➜ Le traitement des données

La data est une mine d'or pour l'entreprise. On parle même de nouvel or noir. Pour que ces données aient effectivement de la valeur, il faut être en capable de les traiter. Et ce, quelle que soit leur nature ou l'emplacement où elles sont stockées.

ÉTAPE 4 : NE PAS OUBLIER L'HUMAIN !

Cela semble couler de source, et pourtant, bien souvent, dans les projets de transformation numérique, la dimension humaine est négligée. Certaines organisations sont tellement focus sur les aspects techniques et technologiques, que les ressources humaines sont laissées au second plan. Et c'est souvent la principale cause d'échec.

Il est donc essentiel d'impliquer les collaborateurs dans ce projet de transformation. Certains le seront dès la phase de diagnostic et deviendront des sponsors pour le reste des équipes.

➜ La formation des équipes

Qui dit nouveaux outils, dit forcément apprentissage. Il est donc important de mettre en place des sessions de formation régulières. Ces dernières devront tenir compte du niveau de chaque collaborateur. En effet, nous ne sommes pas tous égaux devant les outils digitaux, et, la plupart du temps, ce n'est pas une question d'âge, contrairement à ce que l'on pourrait penser !

➜ Démontrer l'intérêt
Au-delà de former et de démontrer l'intérêt de cette transformation pour l'entreprise, il sera important de mettre en avant les avantages pour les collaborateurs eux-mêmes. L'adhésion à ces nouvelles solutions sera ainsi renforcée.

ÉTAPE 5 : MESURE DES RESULTATS ET DEMARCHE D'AMELIORATION CONTINUE

Bien entendu, le projet de transformation ne s'arrête pas au déploiement des solutions. Il est important de mesurer et de comparer avec les objectifs préalablement fixés.

Cette évaluation se fera sur les indicateurs de performance préalablement définis. Il faudra également veiller à mesurer l'adoption de ces outils par les utilisateurs, leur niveau de satisfaction également. Laisser le champ libre aux collaborateurs pour s'exprimer et, par exemple, faire des suggestions d'amélioration, vous aidera à faire évoluer vos outils, mais aussi à renforcer leur implication dans le projet.

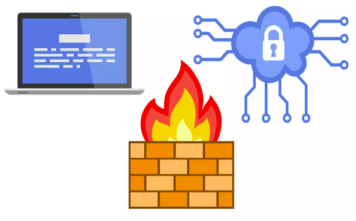
Établir un diagnostic, identifier les besoins, définir comment seront gérées les données, placer l'humain au cœur du projet et mesurer régulièrement les résultats : voici les 5 clés de la réussite d'un projet de transformation numérique.

DOCUMENT 6

Qu’est-ce qu’un pare feu de nouvelle génération ?

RENSEIGNEZ-VOUS SUR LES DIFFÉRENCES ENTRE LE NGFW ET LES PARES-FEU TRADITIONNELS

Archives Factory le : 26 novembre 2020



Les pares-feux sont un outil de sécurité standard pour la majorité des entreprises, mais dans le paysage changeant des menaces d’aujourd’hui, les pares-feux de prochaine génération sont les seuls pares-feux qui peuvent fournir une protection adéquate.

UNE DÉFINITION DU PARE-FEU DE NOUVELLE GÉNÉRATION

Un pare-feu de nouvelle génération (NGFW) est, comme Gartner le définit, un « pare-feu d’inspection des paquets profonds qui va au-delà de l’inspection et du blocage des ports et des protocoles pour ajouter l’inspection au niveau de l’application, la prévention des intrusions et l’apport de renseignements de l’extérieur du pare-feu ».

PARE-FEU TRADITIONNELS VS PARE-FEU DE NOUVELLE GÉNÉRATION

Comme leur nom l’indique, les pares-feux de nouvelle génération sont une version plus avancée du pare-feu traditionnel, et ils offrent les mêmes avantages. Comme les pare-feu réguliers, NGFW utilise à la fois le filtrage statique et dynamique des paquets et la prise en charge VPN pour s’assurer que toutes les connexions entre le réseau, Internet et le pare-feu sont valides et sécurisées. Les deux types de pare-feu devraient également être en mesure de traduire les adresses réseau et portuaire afin de cartographier les adresses IP.

Il existe également des différences fondamentales entre le pare-feu traditionnel et les pares-feux de prochaine génération. La différence la plus évidente entre les deux est la capacité d’un NGFW à filtrer les paquets en fonction des applications.

Ces pares-feux ont un contrôle et une visibilité étendus des applications qu’il est en mesure d’identifier à l’aide de l’analyse et de l’appariement des signatures. Ils peuvent

utiliser des listes blanches ou un IPS basé sur la signature pour faire la distinction entre les applications sûres et les applications indésirables, qui sont ensuite identifiées à l'aide du décryptage SSL.

Contrairement à la plupart des pare-feu traditionnels, les NGFW incluent également un chemin par lequel les futures mises à jour seront reçues.

AVANTAGES DE L'UTILISATION D'UN PARE-FEU DE NOUVELLE GÉNÉRATION

Les caractéristiques différenciantes des pares-feux de nouvelle génération créent des avantages uniques pour les entreprises qui les utilisent.

NGFWs sont en mesure d'empêcher les logiciels malveillants d'entrer dans un réseau, quelque chose que les pare-feu traditionnels ne serait jamais en mesure d'atteindre. Ils sont mieux équipés pour faire face aux menaces persistantes avancées (API). NGFWs peut être une option à faible coût pour les entreprises qui cherchent à améliorer leur sécurité de base, car ils peuvent intégrer le travail des antivirus, pare-feu, et d'autres applications de sécurité dans une solution. Les caractéristiques de ceci incluent la sensibilisation d'application, les services d'inspection, aussi bien qu'un système de protection et un outil de conscience qui bénéficient à l'offre à toutes les chances.

L'IMPORTANCE DES PARE-FEU DE NOUVELLE GÉNÉRATION

L'installation d'un pare-feu est une exigence pour toute entreprise.

Dans l'environnement d'aujourd'hui, avoir un pare-feu de nouvelle génération est presque aussi important.

Les menaces qui pèsent sur les appareils personnels et les grands réseaux changent chaque jour.

Avec la flexibilité d'un NGFW, il protège les appareils et les entreprises contre un spectre beaucoup plus large d'intrusions. Bien que ces pares-feux ne soient pas la bonne solution pour toutes les entreprises, les professionnels de la sécurité devraient examiner attentivement les avantages que les NGFW peuvent offrir, car ils ont un très grand avantage.

DOCUMENT 7

Cloud : à quelles tendances doit-on s'attendre en 2022 ?

EPSI le 15/04/2022

Le marché du Cloud se porte à merveille, comme le prouve une récente étude de Canalys. Cette analyse indique qu'il a connu une croissance de 36 % au deuxième trimestre 2021 par rapport à la même période de l'année précédente. Il a ainsi atteint le seuil des 47 milliards de dollars. Continuant à surfer sur cette vague positive, le Cloud Computing connaît différentes tendances en 2022.

1 Les entreprises tendent à utiliser des environnements multi-Cloud

Dans le passé, les entreprises souhaitant migrer vers le Cloud choisissaient entre trois infrastructures principales :

- Cloud public : un environnement appartenant à un organisme privé qu'une entreprise peut exploiter moyennant un abonnement ;
- Cloud privé : une infrastructure appartenant à l'entreprise elle-même ;
- Cloud hybride : une combinaison des deux univers de Cloud Computing précédents.

En 2022, l'utilisation de plateformes multi-Cloud sera l'option privilégiée. Elles constituent un écosystème informatique dans lequel plusieurs services de cloud public, privé et hybride sont combinés pour répondre aux objectifs organisationnels d'une entreprise. C'est ce que confirme le rapport de Markets and Markets, qui indique que le marché du multi-Cloud connaîtra une croissance de 31 % en 2022, par rapport à 2017.

2 La sécurisation du Cloud est une préoccupation majeure

Il est désormais clair que les entreprises préfèrent stocker leurs informations sur le Cloud. Néanmoins, la migration d'un stockage physique à un autre sur une plateforme de Cloud Computing a son lot de risques.

Par exemple, une erreur humaine peut conduire au stockage de données sensibles sur un service Cloud public. De même, comme ils ne sont pas toujours formés aux bonnes pratiques de la cybersécurité, les employés utilisent parfois des applications en nuage non approuvées. Il arrive même que des identifiants soient partagés sur ces infrastructures non sécurisées.

Pour répondre à cette problématique, il est prévu que les sociétés consacrent un budget plus important pour la sensibilisation contre les risques informatiques, et pour la sécurisation des réseaux Cloud.

Cette tendance est confirmée par une enquête signée The Enterprise Strategy Group, qui confirme que 83 % des organisations entendent allouer un budget plus important aux technologies de sécurité.

3 Le Cloud change le visage de l'environnement professionnel

La pandémie du Covid-19 a fait que les sociétés sont devenues plus résilientes et ont décidé de s'adapter à de nouveaux modes de travail comme le télétravail. Ce passage au travail à distance n'aurait pu aboutir sans des applications Cloud aux multiples usages (solutions Saas, outils collaboratifs…).

Deux ans plus tard, la digitalisation et les modes de travail qu'elle induit sont devenus une norme. Cela est confirmé par l'enquête COVID-19 US Digital Sentiment Survey de McKinsey, qui précise que 75 % des entreprises ambitionnent de poursuivre leur transition numérique pour les années à venir.

Comme le Cloud Computing connaît une évolution constante, il est prévu que ce dernier enregistre un besoin conséquent de cadres spécialisés. Si vous souhaitez faire carrière dans ce domaine au fort potentiel de croissance, vous pouvez suivre les formations proposées par EPSI

DOCUMENT 8

Les grandes tendances de la cybersécurité en 2022

SFR Business le 22/03/2022

En 2021, plus d'**une entreprise sur deux a subi au moins une cyberattaque réussie**. Les cybermenaces de plus en plus nombreuses et complexes s'avèrent toujours plus efficaces pour extorquer les organisations. Plus que jamais, comprendre l'**évolution des attaques informatiques** et des moyens pour s'en prémunir est indispensable pour les entreprises. Tour d'horizon des **principales menaces informatiques** et des **avancées en matière de cybersécurité en 2022**.

Xavier Poinsignon Responsable Offre sécurité mobile

Les 7 principales menaces informatiques en 2022

Les cybermenaces ne représentent pas toutes le même danger pour les entreprises. Nous faisons le point sur les 7 principales menaces informatiques, de la plus répandue à la plus originale.

1. Des ransomwares toujours plus nuisibles

Les ransomwares continuent leur inquiétante progression : ils représentent pas moins de **79% des cyberattaques recensées**, selon Sophos. Les attaques par rançongiciel ont augmenté de 60% sur les 6 premiers mois de 2021, après avoir augmenté de 255 % en 2020, selon les derniers chiffres de l'ANSSI.

En 2022, cette cybermenace évolue et se perfectionne. On observe **la montée en puissance de la double extorsion** : le pirate informatique exige une première rançon pour déchiffrer les données, puis une seconde pour éviter que les données ne soient revendues sur le dark web. Certains analystes mentionnent même l'émergence d'un mécanisme de **triple extorsion** : en plus du chiffrement et de la menace de revente des données, les cybercriminels réalisent des attaques DDoS pour accentuer la pression sur la victime. Ces pratiques pourraient faire jusqu'à deux fois plus de victimes en 2022, selon une étude de la start up Anozr Way.

2. Des attaques DDoS en constante augmentation

Tout comme les rançongiciels, les **attaques par déni de service distribué (DDoS)** visent à bloquer l'infrastructure de l'entreprise. Le cybercriminel envoie des millions de requêtes simultanément vers une cible. Le volume de connexion est si important que le serveur visé ne peut répondre et finit par devenir indisponible.

Les attaques DDoS telles qu'on les connaît aujourd'hui existent depuis plus de 20 ans. Mais on assiste actuellement à une démultiplication et une complexification de ce type de menaces. Fait marquant : la **surface d'attaque** des Systèmes d'Information étant à la fois plus étendue et diversifiée, il est logiquement plus simple aujourd'hui de générer des attaques distribuées

depuis de nombreux équipements compromis disponibles sur Internet. Certains chiffres parlent d'eux-mêmes : AWS, l'entité Cloud d'Amazon, a dû contrer une attaque DDoS d'un volume record de 2,3 Tbps. Certaines études montrent que l'utilisation de la bande passante pour agresser une seule entreprise est en hausse de 49 %, et celui du taux de paquets de 91 %.

3. L'usurpation d'identité (ou "fraude au président") : un classique de la cybersécurité

L'art de se faire passer pour quelqu'un d'autre ne date pas d'Internet. Mais avec le réseau mondial, cette **manipulation** a pris une toute autre dimension. L'entreprise subit dans un premier temps un **vol de données** (via une technique de **phishing** par exemple), afin de récupérer l'identité de collaborateurs. Le pirate, qui peut être à l'autre bout de la terre, se fait alors passer pour un collaborateur afin de demander un règlement urgent. Croyant avoir affaire à une demande légitime, la personne sollicitée s'exécute.

Les fraudes aux faux présidents et aux faux fournisseurs figurent parmi les cybermenaces les plus en vogue. Et nombreuses sont les entreprises qui en ont été victimes : 2 sur 3 ont subi au moins une tentative de fraude en 2021. Nul doute que l'usurpation d'identité est toujours à prendre au sérieux en 2022.

4. Toujours plus de failles Zero Day

Les failles informatiques non résolues mais immédiatement exploitées par les hackers touchent bon nombre d'applications utilisées par l'entreprise. Ces failles sont difficiles à contrer car méconnues. Dès leur identification, il est indispensable d'appliquer les **correctifs de sécurité** publiés par le fabricant ou d'utiliser des **sondes de détection**. 2021 a battu le record de failles découvertes, et 2022 devrait le battre à nouveau.

5. Les attaques contre la supply chain en hausse de 300 %

Les attaques contre les chaînes d'approvisionnement sont un nouveau type de menaces informatiques ciblant la logistique des entreprises, jusque-là ignorée par les cybercriminels. Les tensions liées aux pénuries de composants électroniques et de matières premières (accentuées par le contexte géopolitique) mettent encore plus sous tension les entreprises qui travaillent déjà en flux tendu.

Les cybercriminels l'ont bien compris et cherchent à désorganiser la chaîne d'approvisionnement déjà fragilisée afin de paralyser la production de l'entreprise et se mettre ainsi en position d'exiger une rançon. Ces attaques ont été multipliées par 300 % entre 2020 et 2021. Tout porte à croire que ce type d'attaque va continuer de progresser en 2022.

6. Croissance de l'IoT : une surface d'exposition augmentée

L'IoT est un secteur en pleine croissance et son potentiel est considérable, notamment dans le secteur industriel. En 2022, plus de 12 milliards d'objets sont reliés à internet, selon le cabinet IoT Analytics. Or, un grand nombre d'entre eux ne possède pas de sécurité intégrée, notamment dans le secteur de l'industrie et de la santé. Autrement dit, les objets connectés non sécurisés sont autant de portes d'entrée vers le SI des entreprises : une aubaine pour les

hackers ! En 2021, le volume et la surface d'attaque utilisant des **malwares IoT** ont augmenté de 700 %, d'après un rapport Zscaler. Cette tendance est attendue à la hausse pour 2022.

7. Les attaques dopées par l'intelligence artificielle

Les pirates informatiques font de plus en plus appel à **l'intelligence artificielle (IA)** pour repérer les cibles et automatiser les attaques de manière encore plus massive. C'est pour eux un véritable gain de temps et d'argent ! L'IA les aide à développer des malwares et des scripts intelligents d'infection et de phishing, à contourner les filtres de sécurité, et à gérer et étendre des **réseaux de botnets** (machines zombies). En 2021, les botnets auraient participé à plus de 2,8 millions d'attaques DDoS. Alors que les menaces informatiques sont toujours plus nombreuses, sophistiquées et que la surface d'exposition augmente constamment, de nouvelles technologies émergent pour répondre aux besoins en cybersécurité des entreprises : les cybermenaces évoluent, les moyens de protection aussi !

Les nouveaux moyens de protection du SI

Les nouveaux moyens de protection renforcent la surveillance du SI. L'architecture SASE et le SOC Nouvelle Génération représentent deux avancées importantes en matière de cybersécurité. En offrant une meilleure protection des terminaux, du réseau physique et des serveurs distants, ces solutions s'adaptent aux évolutions du SI des entreprises.

SASE : la gestion centralisée de la cybersécurité dans le Cloud

En matière de cybersécurité, **la complexité est un facteur de risque**. Alors que la transformation digitale des entreprises ne cesse de faire évoluer le SI des entreprises, celles-ci ont de plus en plus recours aux services de nombreux fournisseurs de cloud pour stocker leurs données et applications métiers. Il en résulte une augmentation de la surface d'exposition et une complexité accrue de la gestion de la cybersécurité : le risque cyber augmente.

Face à cette évolution, le Secure Access Service Edge (SASE, prononcez "SASSI") s'impose comme la grande tendance cybersécurité de 2022. La promesse du SASE est simple : **gérer toute la cybersécurité de votre entreprise depuis une plateforme Cloud unique.**

Le SASE regroupe un ensemble de technologies innovantes de cybersécurité et de réseau, pilotées depuis une interface de gestion centralisée. Parmi ces technologies, on citera notamment les 3 outils de sécurité réseau suivants :

- La passerelle web sécurisée de nouvelle génération NG SWG (Next Gen Secure Web Gateway) vise à protéger le trafic web et cloud (filtrage Web, antivirus, DLP, pare-feu) ;
- Le CASB (Cloud Access Security Broker) sécurise les applications SaaS et IaaS de l'entreprise ;
- La technologie ZTNA (Zero Trust Network Access) traite les connexions entre collaborateurs autorisés à accéder à des applications spécifiques.

En résumé, le SASE est idéal pour permettre à votre entreprise de réussir sa migration vers le Cloud ou gérer un parc très hétérogène de télétravailleurs ou nomades internationaux tout

en garantissant la sécurité des données et applications depuis une seule console de gestion. En simplifiant l'organisation de vos infrastructures, vous définissez efficacement votre politique de sécurité pour l'ensemble de vos utilisateurs et réduisez ainsi votre exposition aux risques.

EDR/XDR et SOC Next Gen : une évolution des outils pour faire face aux nouvelles menaces

EDR et XDR : La protection des terminaux, et plus encore

Face à l'évolution des cybermenaces, les solutions **EPP (Endpoint Protection Platform)** - souvent appelées "antivirus next-gen"- montrent leurs limites. Certes, elles bloquent les attaques de phishing et une grande partie des malwares, mais les pirates sont aujourd'hui en mesure de les contourner.

L'EDR (Endpoint Protection & Response) offre une protection avancée des terminaux (PC, serveurs, tablettes, smartphones…). En effet, dans son volet "détection", il surveille et collecte en continu les données issues des équipements afin de détecter des tentatives d'attaques et d'exploitation de failles. Ensuite, dans son volet "investigation", l'EDR analyse les données collectées afin d'identifier les irrégularités. Enfin, l'EDR envoie les informations nécessaires pour stopper la menace et prévenir toute tentative d'infection.

Le XDR (Extended Detection Response) représente l'évolution naturelle de l'EDR. En plus de tous les terminaux de l'entreprise, le XDR étend sa surveillance à des points d'accès tels que le Cloud, aux réseaux, aux emails, etc. Nul doute que ce type de protection globale va convaincre de plus en plus d'entreprises en 2022.

Le Next Gen SOC : tour de contrôle nouvelle génération

Le SOC (Security Operation Center) est historiquement la tour de contrôle du SI de l'entreprise. Son rôle consiste à détecter, alerter et fournir un rapport détaillé de tout incident de sécurité, pour la réaction à l'incident, il doit ensuite passer la main à une autre équipe, pouvant ajouter du délai dans le traitement. Permettant une approche de sécurité informatique totalement sur mesure, le SOC est assez complexe à installer et maintenir dans le temps et représente un coût non négligeable, même pour les structures importantes.

En 2022, le SOC évolue et gagne en agilité et en réactivité. Désormais accessible aux entreprises de taille plus intermediaire (à partir de 500 postes), le SOC Next Gen démarre d'une base d'un parc PC et Serveurs surveillés par un EDR puis s'étend à d'autres composants clefs constituant le SI (XDR, Pare Feu, Mails, Proxy, IPS) . En plus de l'aspect veille/détection, le **SOC de nouvelle génération** a également la capacité de réagir de manière automatisée et immédiate afin de contrer plus efficacement la propagation d'un malware au sein d'un système d'Information. Un must pour les entreprises qui veulent bénéficier d'une cybersécurité optimale en 2022.

DOCUMENT 9

Qu'est ce qu'un Antivirus de Nouvelle Génération (NGAV) ?

Crowdstrike le 24/03/2022

Un antivirus de nouvelle génération (NGAV, Next-Generation Antivirus) **combine intelligence artificielle, détection des comportements, algorithmes de Machine Learning et atténuation des exploits, afin d'anticiper et de prévenir immédiatement toutes les menaces, connues comme inconnues.** Les NGAV sont basés dans le cloud, ce qui permet de les déployer en quelques heures plutôt qu'en plusieurs mois, tout en supprimant la charge de travail liée à la maintenance des logiciels, à la gestion de l'infrastructure et à la mise à jour des bases de données de signatures.

Les NGAV constituent l'étape suivante en matière de protection des endpoints grâce à une approche sans signature capable de protéger les endpoints de manière plus complète et plus efficace que les antivirus d'ancienne génération.

2022 CrowdStrike Global Threat Report

Nouvelle génération contre ancienne génération

	Antivirus de nouvelle génération	**Antivirus d'ancienne génération**
Détection des menaces inconnues	✓ Combine intelligence artificielle, détection des comportements, algorithmes de Machine Learning et atténuation des exploits.	**X** S'appuie sur des signatures difficiles à mettre à jour et inefficaces contre les attaques sans fichiers.
Impact sur les endpoints	✓ L'architecture cloud n'a aucun impact sur les performances des endpoints ou ne nécessite aucun logiciel ou matériel supplémentaire.	**X** Les analyses et mises à jour mobilisent un volume important de ressources et ralentissent les endpoints.
Délai de rentabilité	✓ Implémentation en quelques heures	**X** Implémentation en plusieurs mois

Détection des menaces connues et inconnues

Les antivirus d'ancienne génération utilisent des chaînes de caractères appelées « signatures » et associées à des types spécifiques de malwares afin de détecter et de

prévenir de nouvelles attaques similaires. **Cette approche est en passe de** devenir obsolète dans la mesure où les cyberattaquants les plus ingénieux ont trouvé de nouvelles manières de contourner les protections assurées par les antivirus d'ancienne génération, notamment en lançant des attaques sans fichiers utilisant des macros, des moteurs de scripts, des chargeurs en mémoire, des commandes d'exécution, etc. On estime qu'en 2019 les attaques sans fichiers représentaient 38 % de toutes les attaques. En outre, les antivirus d'ancienne génération basés sur des signatures et l'heuristique ne détectent que 57 % de toutes les attaques potentiellement dangereuses.

Les antivirus d'ancienne génération contraignent les entreprises à adopter une approche réactive et les protègent uniquement contre les malwares et les virus connus répertoriés dans la base de données du fournisseur de l'antivirus. Cette approche était ce qui se faisait de mieux par le passé, mais est tout simplement inadéquate aujourd'hui pour lutter contre les menaces inconnues avec la même rigueur. Selon une étude menée par le Ponemon Institute, 76 % des participants ayant été victimes d'une compromission indiquent qu'il s'agissait d'une attaque zero day nouvelle ou inconnue. Seuls 19 % des participants victimes d'une compromission ont été en mesure de relier cette compromission à une menace connue.

Les antivirus de nouvelle génération ne souffrent pas de ces limitations, car ils tirent parti de méthodes de prévention plus sophistiquées (comme le Machine Learning, la détection des comportements et l'intelligence artificielle) qui permettent de ne pas s'appuyer uniquement sur des signatures pour détecter les activités malveillantes. Les NGAV protègent aussi bien contre les menaces inconnues que contre les menaces connues, ce qui est de plus en plus important au vu de l'augmentation des attaques sans fichiers. Ils permettent d'exposer en temps quasi réel ces deux types de menaces et sont bien plus efficaces et rapides que les antivirus d'ancienne génération dès lors qu'il s'agit d'aider les entreprises à les bloquer.

Délai de rentabilité

Les antivirus d'ancienne génération sont également à la traîne en termes de délai de rentabilité, avec un temps de déploiement moyen de trois mois. Ce délai s'explique par le fait que ces antivirus nécessitent souvent l'installation d'un matériel spécifique sur site. De plus, une fois installées, la plupart des solutions traditionnelles doivent être adaptées et configurées pour être pleinement opérationnelles.

Le déploiement d'un véritable antivirus de nouvelle génération natif au cloud est beaucoup plus simple et son implémentation complète peut se faire en quelques heures. Cet antivirus étant basé dans le cloud, il n'y a aucun logiciel ni matériel supplémentaire à acquérir, aucune infrastructure à mettre en œuvre, aucune solution à concevoir et aucune maintenance ni mise à jour des signatures à réaliser régulièrement.

Impact sur les endpoints

Une fois opérationnel, un antivirus d'ancienne génération peut représenter un encombrement important sur les endpoints en raison de l'intégration inefficace de fonctionnalités de sécurité au fil du temps, qui se traduit par des technologies redondantes et une incidence négative sur les performances. Le fait que son efficacité soit conditionnée à l'utilisation de signatures implique que les bases de données de signatures doivent être mises à jour en permanence

pour inclure les derniers ajouts. Ces mises à jour consomment un volume considérable de données et demandent un temps tout aussi important, sachant qu'à peine une mise à jour terminée, elle est déjà obsolète.

Les antivirus de nouvelle génération sont conçus pour utiliser un agent léger unique, qui mobilise très peu de ressources et n'a qu'un impact minimal sur les endpoints.

Qu'attendre d'un antivirus de nouvelle génération ?

Un antivirus de nouvelle génération efficace doit s'appuyer sur des technologies innovantes pour faire face à des cyberadversaires qui changent constamment de tactiques, techniques et procédures pour s'infiltrer dans les entreprises, qu'il s'agisse de malwares de base ou zero day, ou encore d'attaques avancées sans logiciels malveillants. Les fonctionnalités de prévention à privilégier sont les suivantes :

1. Prévention des logiciels malveillants connus et inconnus

a. Protection antimalware sans fichiers de signatures

La protection antimalware sans fichiers de signatures utilise des algorithmes de Machine Learning pour déterminer la probabilité qu'un fichier soit malveillant. Les nouvelles menaces sont bloquées en temps réel et la rentabilité est immédiate.

b. Machine Learning

Le Machine Learning peut détecter et contrer les logiciels malveillants connus et inconnus, que les endpoints soient connectés au réseau ou non. Il détecte les indicateurs d'attaque de manière plus rapide et précise, élimine les ransomwares et comble les failles laissées par les antivirus d'ancienne génération.

2. Prévention des attaques sans logiciels malveillants

a. Indicateurs d'attaque

Les indicateurs d'attaque mettent en corrélation les événements se produisant au niveau des endpoints afin de détecter les activités furtives, signes d'intentions malveillantes. Une solution s'appuyant sur une analyse hors ligne rétrospective pour identifier les indicateurs d'attaque est incapable de rester au fait des dernières cybermenaces, en plus de nécessiter des ressources considérables. Les algorithmes en ligne qui exploitent le Machine Learning et n'ont pas besoin d'un ensemble complet de données pour effectuer des analyses pertinentes sont à la fois plus rapides, plus efficaces et plus performants.

b. Blocage des exploits

Les malwares ne sont pas toujours distribués au moyen de fichiers. Les attaques basées sur des macros, des commandes d'exécution, des chargeurs en mémoire et d'autres techniques sans fichiers sont en effet de plus en plus courantes. Le blocage des exploits permet de détecter et de bloquer les exploits dès qu'ils se produisent.

3. Intégration de la cyberveille

L'intégration de la cyberveille permet de déterminer immédiatement l'origine, l'impact et la gravité des attaques dans l'environnement et apporte les conseils nécessaires pour une intervention décisive et une résolution rapide.

4. Solution native au cloud

L'architecture cloud est une composante fondamentale des antivirus de nouvelle génération. Un NGAV basé dans le cloud peut être totalement opérationnel en quelques secondes, et ce sans redémarrage, mise à jour des signatures, configuration ni acquisition d'une nouvelle infrastructure. Les algorithmes peuvent traiter en direct l'activité des endpoints et exposer les fichiers malveillants et les comportements suspects en temps quasi réel, sans incidence sur les performances des endpoints.

Fonctionnement d'un antivirus de nouvelle génération

Les antivirus de nouvelle génération exploitent de nouvelles technologies pour assurer la protection des endpoints d'une manière radicalement différente des antivirus traditionnels. Tirant parti d'algorithmes de Machine Learning sur une architecture cloud, les NGAV peuvent neutraliser les menaces en constante évolution qui sont aujourd'hui si répandues.

Un antivirus de nouvelle génération présente les caractéristiques suivantes :

1. Agent léger unique

Grâce à une architecture cloud et à un agent léger unique, l'impact sur les endpoints est quasiment nul, ce qui évite de sacrifier les performances au profit de la sécurité.

2. Fonctionnalités de prévention de haut niveau

Un véritable antivirus de nouvelle génération s'appuie sur des outils et méthodes de prévention sophistiqués qui bloquent non seulement les malwares, mais aussi les attaques sans fichiers, quelles que soient les tactiques, techniques et procédures utilisées par les cyberattaquants. Ces outils et méthodes incluent notamment le Machine Learning, le blocage des exploits, les listes blanches et noires personnalisées, les indicateurs comportementaux d'attaque, l'attribution de la responsabilité des attaques et le blocage des adwares.

3. Aucune mise à jour des signatures nécessaire

Le Machine Learning permet de tirer parti d'algorithmes sophistiqués pour analyser des millions de caractéristiques de fichiers en temps réel et déterminer si un fichier est malveillant.

Comme elles ne s'appuient pas sur des signatures, les solutions NGAV telles que CrowdStrike Falcon sont capables de détecter et de bloquer à la fois les malwares connus et inconnus, même lorsque les endpoints ne sont pas connectés au cloud.

4. Prévention en ligne et hors ligne

L'agent intelligent CrowdStrike Falcon prévient les menaces aussi bien en ligne qu'hors ligne et prend en charge le traitement des données et la prise de décision au niveau de l'endpoint. De cette façon, vous bénéficiez non seulement d'une détection et d'une prévention de haute précision, mais aussi d'une protection continue des endpoints, qu'ils soient en ligne ou hors ligne.

5. Rentabilité immédiate

Les solutions NGAV sont généralement déployées et opérationnelles en quelques heures, sans matériel ni logiciel supplémentaire et sans réglage ni configuration. Certains clients indiquent avoir installé jusqu'à 70 000 agents en une seule journée.

6. Aucune charge de gestion

Les solutions NGAV sont conçues pour s'intégrer de façon transparente dans les environnements sans introduire de complexité supplémentaire. En outre, aucune infrastructure de gestion sur site n'est nécessaire.

7. Intégration

Les solutions NGAV s'intègrent en toute facilité aux solutions SIEM. Grâce aux capteurs Falcon de CrowdStrike qui extraient les événements collectés depuis les endpoints et aux API Falcon qui s'intègrent aux renseignements fournis par des sources tierces et aux indicateurs de compromission existants, les entreprises peuvent tirer le meilleur parti possible de leurs investissements de sécurité.

DOCUMENT 10

L'offre Cloud Computing de l'UGAP : un nouveau marché pour accélérer la transformation digitale du service public

UGAP le 24 janvier 2022

En partenariat avec la Direction des Achats de l'État (DAE) et la Direction Interministérielle du numérique (DINUM), l'UGAP a notifié son premier marché Cloud en mai 2020. Objectif : proposer une solution simple aux collectivités pour garantir leur transition numérique.

Un vrai atout pour les services publics

« Ce nouveau marché s'inscrit dans la volonté de l'UGAP d'accompagner ses clients dans leur transformation numérique » explique Palisakd Nakhonevongsakd, chef de produit référent infrastructures à l'UGAP. Mais de quoi s'agit-il ? L'informatique en nuage, ou Cloud computing, est une technologie qui permet un accès instantané à des infrastructures ou à des services numériques consommés à l'usage (messagerie électronique, calcul haute performance, sauvegarde, base de données, développement de logiciels…) via Internet (le ''cloud'' ou ''nuage'') à partir d'un fournisseur. « La stratégie Cloud de l'État encourage aujourd'hui les acteurs publics à se saisir de son potentiel pour développer une nouvelle génération de services flexibles, modulaires et accessibles. Autrement dit, ce marché est un outil essentiel pour accélérer la transformation digitale des collectivités » souligne l'expert de l'UGAP. En se dotant d'un service Cloud Computing, les collectivités garantissent ainsi leur transition numérique et optimisent leurs démarches internes et externes, le tout en maîtrisant la sécurité de leurs données. « Via son offre Cloud Computing, l'UGAP a l'avantage de proposer à ses clients un catalogue de services présélectionnés, adaptés, qualifiés et certifiés notamment SecNumCloud et HDS par les acteurs majeurs du Cloud » détaille Palisakd Nakhonevongsakd.

Des services simples pour des avantages concrets

Dans un secteur qui peut sembler compliqué, l'objectif de l'UGAP est donc de proposer aux collectivités des solutions simples et faciles d'accès. Les services Cloud peuvent avoir des impacts bénéfiques dans divers domaines comme celui de la dématérialisation des démarches administratives par exemple. Le Cloud peut aussi

jouer un rôle dans l'amélioration de l'expérience usager, ou encore dans le développement d'outils de communication ou de collaboration pour les agents. Selon Palisakd Nakhonevongsakd, « le Cloud permet également d'optimiser de la donnée dans l'administration. De nombreux systèmes existent comme ceux liés à l'intelligence artificielle, aux services d'échanges de données, d'open data ou encore simplement d'archivage ». Des enjeux avec lesquels les collectivités doivent composer au quotidien.

Une aide au choix

L'offre de l'UGAP propose des solutions de type IAAS (Insfrastructure as a Service) et PAAS (Platform as a service). « Ces deux solutions proposent un large choix de services pouvant répondre aux différents besoins d'infrastructures des collectivités » assure Palisakd Nakhonevongsakd avant de préciser que « ce qui fait la force de l'offre de l'UGAP c'est qu'elle s'accompagne d'une ''aide au choix'' pour ses clients. Car nous gardons toujours le même objectif : celui d'accompagner au mieux les collectivités dans leur transition numérique ». Enfin, au-delà d'une large palette de services et d'une aide au choix, le récent marché Cloud de l'UGAP permet aussi à ses clients de bénéficier de tarifs préférentiels.

BON À SAVOIR

Il existe deux dispositifs pour aider les collectivités à investir et basculer facilement vers l'utilisation du Cloud.

> Fonds de compensation de la taxe sur la valeur ajoutée (FCTVA)

• Les « dépenses de services d'infrastructure de l'informatique en nuage » ouvriront droit à un taux de compensation forfaitaire, limité à **5,6%**. L'extension au FCTVA ne concerne que ''les prestations de cloud de type **'Infrastructure as a Service' (IaaS)** »
• Le dispositif concerne les prestations de solutions relevant de l'informatique en nuage déterminées par un arrêté interministériel et payées par les collectivités depuis le 1er janvier 2021 (article 69)

> Paiement avant service fait

• Les abonnements et consommations de services informatiques en nuage ''Cloud'' sont dorénavant assimilés aux dépenses de fournitures d'accès à internet et abonnements téléphoniques, **ces dépenses pouvant être payées avant service fait.**
• Ces dispositions sont issues de l'arrêté du 16 février 2015 qui fixe les dépenses des collectivités territoriales, de leurs établissements publics et des établissements publics de santé pouvant être payées sans ordonnancement préalable ou service fait.

DOCUMENT 11

Doctrine Cloud au centre : quel impact pour le secteur public ?

Plateforme WIMI le jeudi 17 février 2022

Ces dernières années, les technologies numériques ont modifié notre façon de travailler. Désormais, dématérialisation des documents, signature électronique, télétravail, outils et applications diverses font partie du quotidien d'une grande partie des entreprises privées ainsi que des organisations publiques en France. C'est ce que l'on appelle la transformation numérique. Et la crise sanitaire n'a fait qu'accélérer la numérisation des services publics afin d'assurer le maintien des activités et des services des administrations, mais aussi pour proposer de nouveaux services aux citoyens.

Aujourd'hui, la plupart de ces services fonctionnent grâce à l'adoption de technologies cloud qui permettent à la fois l'hébergement et le traitement des données des administrations et des citoyens. En 2018, l'État faisait du cloud computing (ou informatique en nuage) l'un des chantiers prioritaires de sa transformation numérique. Et en mai 2021, le gouvernement a annoncé sa politique « Cloud au centre » afin d'encourager l'ensemble des acteurs publics à utiliser le cloud computing pour développer des services numériques de qualité, tout en protégeant au mieux les données des entreprises et des citoyens français.

Découvrez ce qu'est la doctrine « Cloud au centre » et ce que cela implique pour le secteur public.

Qu'est-ce que la doctrine « Cloud au centre » ?

La doctrine « Cloud au centre » fait partie de la stratégie nationale du gouvernement qui vise à « protéger toujours mieux les données des entreprises, des administrations et des citoyens français ». Elle s'inscrit dans la continuité de la doctrine cloud de 2018, et repose sur trois enjeux majeurs pour la France : la transformation des entreprises et des administrations, la souveraineté numérique et la compétitivité économique.

La doctrine « Cloud au centre » concerne tous les acteurs de l'État ainsi que les organismes placés sous sa tutelle. A travers cette doctrine, le gouvernement souhaite que le cloud devienne le mode d'hébergement et de production par défaut des services numériques de l'État. Il veut également montrer l'exemple en matière de protection des données.

Enfin, le passage au cloud doit renforcer la résilience des produits numériques des administrations en cas d'incident, et ainsi garantir la continuité du service public. Le but est de garantir la confiance des Français dans le service public numérique.

Afin d'inscrire durablement le cloud dans la stratégie numérique des administrations, les agents publics seront formés aux technologies du cloud computing et les services numériques des administrations devront être hébergés sur l'un des deux cloud interministériels internes de l'État ou sur des solutions cloud répondant à des critères stricts de sécurité et certifiées SecNumCloud.

Quel est l'impact pour les acteurs du secteur public ?

L'objectif de la doctrine « Cloud au centre », c'est de s'assurer que les administrations publiques se lancent dans une transformation numérique de qualité qui permet de renforcer la souveraineté de l'État ainsi que la protection des données des entreprises et des citoyens français.

Ainsi, pour mettre en œuvre cette doctrine, les acteurs du secteur public doivent opérer un changement de culture, acquérir de nouveaux savoir-faire et adapter leurs modes de fonctionnement et leurs pratiques au quotidien.

Voici ce qui les attend.

Réfléchir autrement

Les équipes informatiques doivent réfléchir en mode cloud, c'est-à-dire que pour tout nouveau projet numérique, elles ne doivent plus fonctionner comme elles le faisaient auparavant, mais elles doivent rechercher une solution cloud. Cela implique un véritable changement de culture et une nouvelle façon de penser.

Pour cela, le gouvernement conseille aux organisations publiques de se faire suivre et accompagner par des experts qui les aideront à maîtriser les outils et à former les équipes aux bonnes pratiques du cloud computing. Les fournisseurs de service cloud peuvent également les assister et leur proposer des formations adaptées.

Recruter et former

Les administrations devront recruter des personnes compétentes et mettre en place des programmes de formation dédiés au cloud pour les agents faisant partie des équipes informatiques ainsi que des directions qui utilisent des produits numériques ou gèrent des projets numériques. Les équipes qui débutent dans ce domaine pourront bénéficier d'un accompagnement spécifique de leur ministère et de la direction interministérielle du numérique (DINUM).

Bien choisir la solution cloud

Le choix de la solution cloud la plus adaptée dépend des différentes contraintes de l'organisation publique (contraintes réglementaires et de sécurité, licences logicielles, etc.) ainsi que du type de données qu'elle traite au quotidien.

Par exemple :

- si l'administration traite des données sensibles (données personnelles, données financières ou bancaires, données confidentielles, etc.), elle devra utiliser le cloud interne ou un cloud commercial digne de confiance (certifié SecNumCloud), sous la protection du droit européen et qui respecte le RGPD ;
- si elle traite des données médicales, l'hébergeur doit, en plus des conditions citées précédemment, être conforme à la législation sur l'hébergement de données de santé;
- si elle gère des données non sensibles, elle pourra utiliser une solution de cloud commercial de son choix, tant que celle-ci répond à des exigences strictes, c'est-à-dire qu'elle soit **qualifiée SecNumCloud et protégée des réglementations hors de l'Union européenne**.

Respecter le budget

Les acteurs du service public qui entreprennent leur transformation numérique et adoptent la doctrine « Cloud au centre » doivent être attentifs à ne pas augmenter leur budget informatique sous prétexte de suivre les objectifs stratégiques de modernisation imposés par le gouvernement.

Ainsi, lorsqu'elles choisissent un fournisseur de cloud computing, les organisations publiques doivent prendre en compte différents critères tels que la garantie d'un haut niveau de sécurité, la conformité avec le RGPD, la politique de contrôle des accès, le chiffrement des données, etc., ainsi que le prix de la prestation.

Pour conclure

Avec la doctrine « Cloud au centre », l'État encourage l'ensemble des acteurs publics à développer un meilleur service public numérique, tout en garantissant la protection des données des entreprises et des citoyens français. Pour adopter cette doctrine, les administrations devront changer leurs pratiques et leur culture, ce qui leur permettra d'utiliser au mieux ces technologies.

Pour en savoir plus, rendez-vous sur le site du gouvernement dédié au numérique.

DOCUMENT 12

Les enjeux de la transition numérique au sein des collectivités

Nepsio Conseil 26 avril 2022

Avec l'évolution massive des usages digitaux dans notre quotidien, la transition numérique est devenue un domaine prioritaire, également au sein des collectivités.

Les services publics font face à de nouveaux enjeux numériques centraux et essentiels, tant de **gouvernance**, **d'organisation** qu'à **l'évolution des besoins des usagers**. Ils se confrontent également à une **réglementation** récente, fixant le cadre et les objectifs numériques pour toutes les collectivités territoriales comme la Loi pour une République numérique du 7 octobre 2016, Loi n° 2016-1321, qui prépare le pays aux enjeux de la transition numérique et de l'économie de demain. Les attentes renforcées des usagers pendant la crise sanitaire ont d'ailleurs incité le gouvernement à mobiliser 1,7 Milliards d'euros pour soutenir la **transformation numérique de l'Etat et des collectivités territoriales** dans le cadre du **plan de relance.** Garantissant **simplicité, rapidité et proximité d'usage**, le numérique et la digitalisation ont le potentiel de devenir de véritables outils renforçant la qualité de la relation entre le service et l'habitant.

Au-delà de cet intérêt évident, ils constituent également une opportunité majeure pour le **maintien de la souveraineté** et de **performance organisationnelle** d'une collectivité. Plus précisément, dans quelle mesure la **maturité numérique** des collectivités relève-t-elle **d'enjeux fondamentaux d'acculturation et de maîtrise de la donnée ?**

Des enjeux de gestion des ressources humaines

Le numérique est non seulement un sujet d'amélioration de la relation aux usagers : c'est aussi un **sujet organisationnel central et de grande ampleur.** Engager la transformation numérique dans une collectivité, c'est engager une transformation en profondeur de l'organisation, en passant tant par une réflexion sur le niveau **d'acculturation au numérique des agents**, que sur ses **méthodes de management** et ses **outils**.

De fait, 60% des agents territoriaux estiment avoir besoin d'être formés au numérique pour améliorer leur autonomie et leur qualité de vie au travail. Ils font face à des transitions **rapides et parfois à marche forcée** qui nécessitent une **compréhension** et une **maîtrise sécurisée et sécurisante** de leur environnement numérique. Une grande majorité des métiers (communication, finances, planification, métiers d'accueil…) est exposée à la **dématérialisation des procédures**. Cela nécessite de fait une montée rapide en compétences. Dans une démarche d'accompagnement RH, tout l'enjeu est donc d'identifier **les besoins et les compétences** les plus pertinentes à mobiliser pour les différents métiers donnés. Ainsi, la capacité d'un service public à adopter de **nouvelles méthodes de travail** (basées par exemple sur l'agilité ou le design thinking) est un déterminant fort de réussite dans ce nouveau contexte.

66% des participants n'ont pas le bagage suffisant pour être en maîtrise sur l'ensemble des situations professionnelles pouvant être vécues sur un poste intégrant une dimension numérique (Pix-2021)

25% sont en grande difficulté (Pix-2021)

Au-delà du développement de nouvelles méthodes de travail, pour une montée effective en compétences, toute démarche de digitalisation des services doit aussi s'accompagner d'une **amélioration des conditions de travail** des agents par **l'accès et l'appropriation de nouveaux outils.** On peut notamment penser aux outils interfacés (entre services ou collectivités) permettant en plus d'une simplification administrative, le développement d'un travail en **transversalité**. Cette digitalisation transverse de la collectivité simplifie de surcroît les processus métiers. Le numérique sert ainsi une boucle vertueuse et la **diffusion de la culture d'un « mode projet »,** qui engendre des réflexions importantes sur la manière dont s'organisent les services (par exemple : modification/ réduction du nombre d'échelons hiérarchiques), et la manière dont sont **réparties et mobilisées les compétences** (développement de la transversalité, souplesse et réactivité…).

Cette stratégie s'intègre également dans un **contexte national** (avec par exemple la sélection de logiciels ou de systèmes de gestion des données français plutôt qu'étrangers, ou en évitant le recours aux GAFAM), mais aussi dans un **contexte européen** (choisir des solutions qui interdisent la sortie des données des habitants hors des frontières de l'UE afin de pouvoir pleinement bénéficier de la protection du RGPD.

Qualifiée par certains de « nouvel or noir », la question de la capacité à **maîtriser, protéger puis valoriser** les données territoriales se pose chaque jour pour une **élaboration viable et pertinente des politiques publiques**. C'est ici tout l'art de l'analyse des données pouvant permettre de mieux appréhender les dynamiques des territoires, de mieux cibler et anticiper les besoins des habitants, et, in fine, de mieux mesurer l'impact des politiques locales.

Ces améliorations vont de **l'organisation des matières premières à celle des équipes, en passant par la maintenance des machines**. Il s'agit de chantiers de longue durée, exercés de manière itérative grâce à des outils comme AX2012.

En effet, il est très important dans ce type de projet de prendre le temps de faire les choses avec habileté et prudence, car les employés doivent s'adapter aux nouveaux moyens de fonctionnement petit à petit, afin que cela fasse partie intégrante de leur travail.

Des enjeux de la maitrise de la donnée et de la souveraineté

Si elle représente une opportunité notable pour la **performance organisationnelle** des collectivités territoriales, la transition numérique représente aussi des enjeux certains en matière de **souveraineté et de maîtrise de la donnée** à plus large échelle.

La souveraineté numérique désigne la capacité à *"maîtriser l'ensemble des technologies, tant d'un point de vue économique que social et politique",* et de "*se déterminer pour avoir sa propre trajectoire technologique*" (Bernard Benhamou). Open data, big data, data center… Les collectivités font face à ces variations puissantes qui redessinent les champs d'actions, les

manières de faire et les attentes des usagers. Le sujet de la maîtrise des données est un enjeu existentiel, en tant que le pouvoir d'action sur le territoire passe par une gestion réussie des données (dont le meilleur exemple reste celui de la Smart City). Du pilotage stratégique du territoire aux interventions des services techniques, la capacité à accéder et valoriser les données devient un enjeu de souveraineté pour les collectivités.

Cet enjeu repose sur **le choix d'outils** qui garantissent au service public qu'il conserve la **maîtrise** à travers le **contrôle de ses propres données et de celles générées par les acteurs** qui parcourent son territoire (usagers, prestataires…). Via le respect des règles RGPD par exemple, elle doit s'assurer que les prestataires (hébergeurs, délégataires de service public…) ne s'approprient ni ne diffusent les données publiques. La souveraineté doit alors permettre à la collectivité de discuter d'égal à égal avec l'ensemble des acteurs du territoire.

Le numérique : un enjeu fondamental pour les collectivités

Le **numérique** s'inscrit comme un **outil clé dans le développement d'une collectivité et de ses services internes.** De surcroît, force est de constater qu'il sert aussi des enjeux **d'accessibilité, d'efficacité et de proximité** pour l'usager, mais aussi **d'attractivité et d'image** des territoires (une transition numérique réussie permettant de faire rayonner auprès des usagers l'image d'une administration modernes, en maîtrise des outils numériques du XXIème siècle.). Pour finir, relever les enjeux de transition numérique au sein d'une collectivité, c'est aussi résolument lutter contre **l'illectronisme numérique** qui touche près de 17% de la population (INSEE). **La lutte contre la fracture numérique (avec les moyens humains, techniques, financiers correspondants)** représente alors un **facteur de succès de la stratégie numérique**.

DOCUMENT 13

SECURITE INFORMATIQUE : le Registre Général de Sécurité

SIEEEN 25 janvier 2022

Le référentiel général de sécurité est pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

- Le RGS (registre général de sécurité) version 2.0 a été publiée par arrêté du Premier ministre du 13 juin 2014. Elle est applicable depuis le 1er juillet 2014.
- Le RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- La loi informatique et libertés : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Homologuer la sécurité de votre système d'information est-il pertinent ?

Le risque zéro n'existe pas, à vous de maitriser le risque en adoptant une démarche d'homologation. Toutes les collectivités, quelle que soit leur taille, sont concernées par la cybermalveillance aux conséquences parfois dévastatrices.

- **Les impacts directs sont :** interruption des services administratifs, inaccessibilité des documents financiers ou administratifs, fuites de données à caractère personnel…
- **Les impacts indirects sont :** coûts financiers de rétablissements des services numériques, l'atteinte à la réputation, les conséquences juridiques…

Outre le fait que vous êtes soumis à la loi RGS de 2010, homologuer la sécurité de votre système d'information est bénéfique pour votre commune sur de nombreux aspects :

- Protection de vos données et celles des administrés que vous traitez, vos services en ligne et votre système d'information et de communication
- Sensibilisation de vos agents aux risques de cybermalveillance ;
- Accroissement de la confiance de vos administrés…

Comment ?

L'homologation détermine les règles permettant aux autorités administratives de garantir aux citoyens et aux autres administrations un niveau de sécurité de leurs systèmes d'information adapté aux enjeux et risques liés à la cybersécurité.

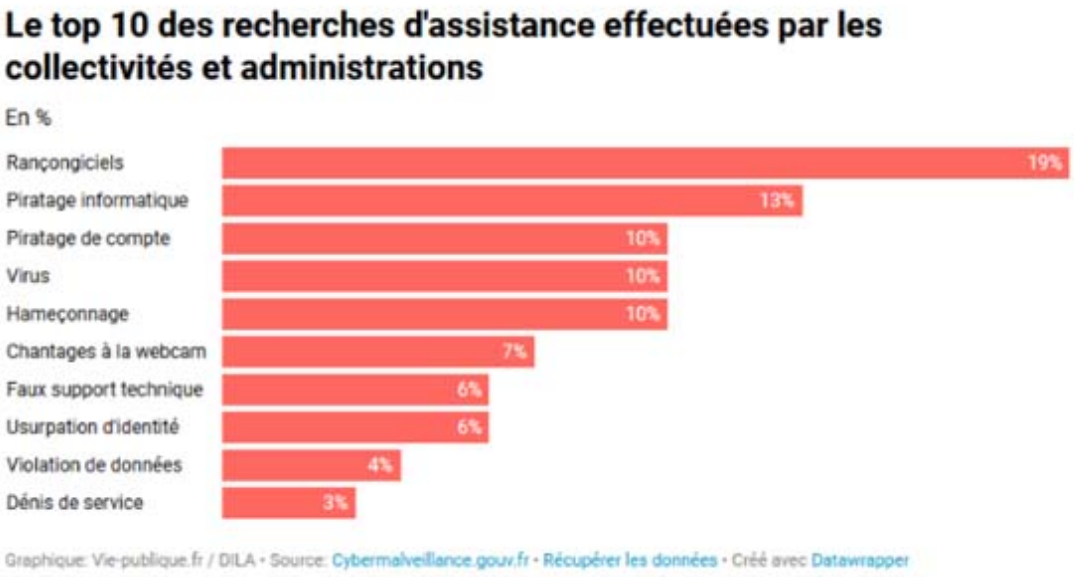
En Cartographiant les données circulant dans votre système d'information et en déterminant la criticité de vos traitements, vous pourriez cibler les actions prioritaires à mettre en œuvre pour protéger vos missions.
A l'issue du diagnostic de sécurité et de l'homologation, vous serez en mesure d'apprécier et de valider votre niveau de risque résiduel.

Vous n'êtes pas à l'abris d'une attaque cyber, n'attendez pas et réagissez maintenant, renforcez votre système d'information !

Chiffres clés :

- **30 % des collectivités territoriales ont été victimes d'un rançongiciel** (Etude du Clusif, juin 2020),
- **192 attaques ont été enregistrées en 2020, avec une rançon de 130.000 euros en moyenne.** Le nombre de cyberattaques a été multiplié par quatre en France en 2020 (Source ANSSI).
- En 2020, **les signalements d'attaques par rançongiciel ont été multipliés par 3,5** par rapport à 2019. Toutes les collectivités sont concernées, quelle que soit leur taille (Source ANSSI).

En 2020 :



Responsabilité des collectivités territoriales :

Les collectivités territoriales sont responsables de la sécurité des données qu'elles traitent et de leurs
services numériques vis-à-vis des autorités et des citoyens.

Quel risque pour la commune en cas de violation de données non déclarée ?

Le fait de ne pas de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende (Article 226-17-1 du code pénal modifié par l'ordonnance n°2018-1125 du 12 décembre 2018).

Exemple de sanction en cas de faille de sécurité :

La CNIL (Délibération CNIL n°2018-003 du 21 juin 2018) a ainsi sanctionné une association en tant que responsable de traitement suite à un incident de sécurité sur son site internet rendant librement accessibles les données personnelles de ses utilisateurs au titre de l'article 34 de la loi du 6 janvier 1978 modifiée, et ce, alors même que le site a été développé par une société prestataire. L'ampleur de la violation (plus de 40 000 documents accessibles) et le degré de sensibilité des données concernées (références bancaires, numéros de sécurité sociale, salaires, passeports...) ont justifié la décision prise par la CNIL de sanctionner l'association à hauteur de 75 000 euros et de rendre publique cette décision.

Pare-feu de nouvelle génération (NGFW)

fortinet.com - consulté le 28 novembre 2022

Présentation

Les pare-feux NGFW FortiGate offrent une sécurité d'entreprise de pointe pour n'importe quel edge, à n'importe quelle échelle, en procurant une visibilité totale et une protection complète contre les menaces. Les entreprises peuvent ainsi intégrer la sécurité dans l'architecture IT hybride et créer des réseaux axés sur la sécurité pour des résultats optimaux :

- Sécurité ultra-rapide, de bout en bout
- Défense cohérente en temps réel grâce aux services FortiGuard
- Excellente expérience utilisateur des processeurs de sécurité dédiés (SPU)
- Efficacité opérationnelle et workflows automatisés

Les pare-feux NGFW FortiGate permettent aux entreprises de concevoir des réseaux performants, ultra-évolutifs et orientés sécurité

Pour éviter que des malwares ne s'immiscent dans votre réseau par le biais du trafic chiffré, vous devez mettre en place des fonctions d'inspection performantes et fiables. Découvrez les performances obtenues par la solution FortiGate 7121F lors de l'un des tests majeurs les plus rigoureux en matière de protection et d'inspection approfondie SSL.

Nouveautés de FortiOS 7.2

Comptant une multitude de nouvelles fonctions et d'améliorations, FortiOS 7.2 offre une puissante combinaison d'informations exploitables optimisées par l'IA, d'automatisation des processus SOC et NOC et de capacités de prévention en ligne visant à contrer les menaces dissimulées et inconnues jusque-là.

Nouveautés de FortiOS 7.2 pour les pare-feux NGFW FortiGate :

- **Prise en charge du protocole HTTP/3 :** L'inspection dans HTTP/3 et QUIC offre une plus grande visibilité, une protection supérieure et une prise en charge des normes émergentes.

- **Unification des règles** : Grâce à la configuration unifiée des règles de pare-feu, toutes les règles sont centralisées à un emplacement unique, y compris l'accès ZTNA.
- **Segmentation des applications SaaS :** Cette fonction permet de protéger les applications SaaS grâce au service CASB en ligne.

Fonctionnalités et avantages

Visibilité totale et contrôle absolu

Bloquez les attaques furtives et par ransomware, ainsi que d'autres menaces dissimulées, grâce à l'inspection des flux sous SSL (TLS 1.3 notamment) et à la protection automatique contre les menaces.

SERVICES DE SÉCURITÉ FORTIGUARD

Consolidez et exécutez simultanément les services de sécurité IPS, DNS et de filtrage Web et vidéo, afin de réduire les coûts et de gérer les risques.

Proxy intégré en natif

En adoptant FortiClient, vous offrirez une expérience utilisateur et une sécurité transparentes aux équipes hybrides grâce à l'accès réseau ZTNA (Zero Trust Network Access).

Sécurité hyperscale

Concevez des réseaux orientés sécurité ultra-évolutifs pour répondre aux exigences croissantes de l'entreprise.

Intégration dans la Security Fabric

Partagez des informations de veille décisionnelle sur les menaces couvrant l'ensemble de la surface d'attaque, afin de mettre en place une infrastructure de sécurité cohérente et coordonnée de bout en bout.

Gestion automatisée du réseau

Mettez en place des opérations efficaces à grande échelle grâce à une console de gestion centralisée simple d'emploi.

Cas d'utilisation des pare-feux NGFW FortiGate

Sécuriser les systèmes hybrides et multi-clouds

Intégrez profondément la sécurité dans les réseaux de data center hybrides, afin de protéger n'importe quel edge, à n'importe quelle échelle, en mettant en place une sécurité de bout en bout sur différents clouds.

Segmentation et prévention de la propagation latérale

Empêchez la propagation latérale, gérez les risques internes et renforcez la sécurité quel que soit le type de segmentation, qu'il soit basé sur VXLAN, le réseau, les endpoints ou les applications. L'intégration dans Fortinet Security Fabric vous offre une confiance dynamique et une segmentation au niveau des ports.

Gestion des vulnérabilités et blocage des menaces

Protégez vos sites contre les attaques connues et de type « zero-day », et bénéficiez de correctifs virtuels avec le service FortiGuard IPS inclus.

PROTÉGER LES UTILISATEURS ET LE PÉRIMÈTRE

Bénéficiez d'une visibilité totale : détectez et corrigez les ransomwares et autres menaces dissimulées dans le trafic HTTPS sans impacter les performances.

ARCHITECTURES HYPERSCALE SÉCURISÉES

Mettez en place une sécurité hyperscale efficace, sans impact sur le réseau, afin de répondre aux exigences croissantes de l'entreprise.

SÉCURISER LES ENVIRONNEMENTS INDUSTRIELS ET OT

Déployez une véritable sécurité d'entreprise pour les environnements OT (Operational Technology) en mettant en place des pare-feux NGFW FortiGate Rugged. Bénéficiez d'une visibilité totale sur le réseau et d'une protection contre les menaces.

La sécurité au cœur du réseau

Les stratégies de sécurité traditionnelles ne peuvent pas suivre le rythme imposé par l'expansion de votre surface d'attaque, qu'il s'agisse du télétravail, de la mobilité ou des réseaux multi-clouds. **La stratégie « Security-Driven Networking » (sécurité au cœur du réseau) de Fortinet** relève ces défis en intégrant étroitement l'infrastructure réseau à l'architecture de sécurité, afin d'assurer la sécurité au cœur de votre réseau au fur et à mesure de son évolution.

DOCUMENT 15

Cybersécurité : l'Anssi veut renforcer son appui aux collectivités territoriales

Banque des territoires le 17 octobre 2022

Dans une intervention aux assises de la cybersécurité de Monaco, le patron de l'Anssi a convenu de l'approche trop "parisienne" de l'agence. Avec la mise en œuvre de centres (CSIRT) régionaux, le financement d'outils et la facilitation de l'homologation des services numériques publics, l'agence promet de mettre la cybersécurité à la portée de toutes les collectivités.

Sur le départ, le directeur de l'Anssi s'est livré, malgré ses propres dénégations, à un mea-culpa sur la stratégie de l'agence en matière de cybersécurité. "Nous avons commencé par les acteurs critiques sans sortir du périphérique parisien", a convenu Guillaume Poupard devant les participants aux assises de la cybersécurité à Monaco, le 12 octobre 2022. Il aura fallu la crise sanitaire, le développement massif du télétravail et la multiplication de cyberattaques affectant hôpitaux et collectivités pour que l'agence infléchisse sa stratégie en 2021. C'est ainsi que 626 collectivités territoriales et hôpitaux (chiffres de juillet 2022) ont bénéficié d'un "parcours cyber" financé dans le cadre du plan de relance (notre article du 21 octobre 2022). Mais ce programme n'a là encore concerné que de grandes collectivités, à l'exception de quelques structures de mutualisation tournées vers les petites communes, l'agence faisant de l'existence d'un responsable de la sécurité des systèmes d'information (RSSI) un préalable à tout accompagnement.

Arrivée de la directive NIS2

Aujourd'hui la stratégie atteint cependant ses limites, les cybercriminels visant le maillon faible (usagers, petites structures…) dans des systèmes administratifs de plus en plus connectés et interdépendants. Face à ce risque systémique, le directeur de l'Anssi plaide pour un 'changement d'échelle' en apportant à chacun - citoyens, TPE-PME, collectivités… - "les moyens de se protéger et d'être protégé". Pour atteindre cet objectif, le premier levier mis en œuvre est la réglementation jugée "efficace si elle est bien utilisée". C'est ainsi que la directive NIS2, texte européen auquel l'Anssi a beaucoup contribué, va élargir à tous les secteurs critiques les obligations cyber : désignation d'un RSSI, notification systématique des incidents, plan de mise en conformité... Si l'on sait d'ores et déjà que les administrations locales seront impactées, il reviendra au législateur de lister précisément les entités concernées.

12 CSIRT en place

La seconde piste consiste à territorialiser la prévention cyber. C'est le rôle des Computer security incident response team (CSIRT) régionaux. "Aujourd'hui nous avons contractualisé avec 12 régions sur 13", s'est félicité Guillaume Poupard. Ces centres, accompagnés à hauteur d'un million d'euros par l'Anssi, ont vocation à mener des actions de sensibilisation, à relayer les alertes et à partager des expériences. L'agence reconnait par ailleurs que ses guides et autres recommandations techniques ne sont pas adaptés aux petites structures. "Quand on vient les voir et qu'on leur dit la base c'est une analyse de risque on les a déjà perdus", concède Guillaume Poupard. Sans compter que le plan d'action qui en découle représente souvent des montants que les collectivités rechignent à engager. Un constat qui a conduit l'agence à changer d'approche en acceptant de financer des outils de protection (notre article du 29 mars 2022) à partir du moment où une structure locale cofinance et anime le programme. Lauréat de cet appel à projets, le syndicat mixte La fibre 64 vient par exemple de lancer son "bouclier cyber64" à destination des communes des Pyrénées-Atlantiques. A l'issue d'un parcours en quatre étapes, les communes et EPCI vont être dotées gratuitement et pendant trois ans d'antispam, d'anti-virus, de gestionnaire de mots de passe et de sauvegarde en ligne.

Lancement du service « MonServiceSécurisé »

Par ailleurs, l'agence finalise la plateforme MonServiceSécurisé, une startup d'Etat chargée d'accompagner la mise en œuvre du décret 2022-513 du 8 avril 2022. Cette réglementation oblige l'ensemble des entités administratives à homologuer leurs services numériques (sites, applications, API, formulaires…) dès lors qu'ils traitent des données d'usagers. Concrètement, elle permettra de calculer simplement un "indice cyber", une évaluation indicative du niveau de sécurité d'un téléservice, qu'il soit en développement ou en ligne, et de suivre étape par étape son processus d'homologation. Enfin, en matière de prévention, Guillaume Poupard avoue qu'il y a "un gros effort à faire". Rappelant que tous les citoyens sont concernés, il appelle à mieux faire connaitre la plateforme "Cybermalveillance". Le GIP intervient désormais sur la sensibilisation, l'aide au diagnostic en cas de piratage et l'appui à la sécurisation des systèmes d'information avec, parallèlement aux ressources grand public, des contenus calibrés pour les petites collectivités.

DOCUMENT 16

Cybersécurité : premier bilan pour l'accompagnement des collectivités

La Gazette des communes ; Publié le 13/06/2022

Après la recrudescence de cyberattaques, l'heure est à la consolidation de la sécurité informatique. Pour les collectivités, cela passe principalement par deux axes : garantir leur propre sécurité et accompagner les entreprises locales. Premier bilan à l'occasion du Forum international de cybersécurité, qui se tenait du 7 au 9 juin à Lille.

Après le temps des attaques et du constat, vient celui de la mise en œuvre des protections. Les dernières années ont été marquées par une recrudescence d'attaques informatiques touchant les collectivités territoriales. Toutes ne partaient pas avec les mêmes armes.

Pour les accompagner dans leur sécurisation et les outiller, l'Etat a missionné l'Anssi, agence de sécurité informatique de l'Etat, dans le cadre du plan de relance. Preuve de l'intérêt pour les différentes offres proposées, le budget accordé de 136 millions a été rallongé de 40 millions supplémentaires, qui doivent être dépensés en 2022.

« Face à une menace cyber toujours grandissante, nous devons plus que jamais faire de la cybersécurité l'affaire de tous. Au niveau local comme national, l'écosystème cyber doit se mobiliser afin de rehausser l'exigence générale de sécurité », a rappelé Guillaume Poupard, patron de l'Anssi à l'occasion du Forum international de cybersécurité (FIC), qui se tenait à Lille du 7 au 9 juin.

Parcours d'accompagnement : Ainsi, plus de 600 collectivités ont participé à des parcours d'accompagnement chapeauté par l'Anssi, avec à la clef un audit identifiant les différentes actions à mettre en œuvre pour garantir une sécurité au maximum. La difficulté pour les collectivités peut être ensuite de trouver les bons interlocuteurs. Pour ce faire, l'Anssi met en avant la labellisation des experts, par le biais de visa.

C'est notamment pour cette raison qu'Hexatrust, qui fédère les entreprises de la filière a réalisé, un catalogue de ses prestataires à destination des collectivités, partagé la première fois au FIC. L'objectif de ce « guide capacitaire » est de les guider dans leur choix des prestataires. Pour chaque entreprise, les différents labels ou partenariats sont rappelés, ainsi que ses principaux champs de compétence.

Renforcer les écosystèmes locaux : L'identification des acteurs est pertinente à plusieurs niveaux localement. Tout d'abord, dans le cadre des missions de développement économique des régions, ainsi que le rappelait les stands installés par plusieurs régions au FIC, telles que les Hauts-de-France, la Nouvelle-Aquitaine, la Bretagne ou encore l'Occitanie. Elles avaient invité les acteurs locaux de la cybersécurité qui pouvaient ainsi présenter leurs services.

« Les centres régionaux permettent de structurer l'écosystème localement », confirme Gwenaëlle Martinet, cheffe de projet à l'Anssi et pilote du volet cyber du plan de relance. « Nous avons de nombreuses entreprises en France, qui proposent des produits répondant à des besoins en matière de sécurité numérique. Un des défis du plan de relance, c'est de faire en sorte que ces produits soient déployés et d'aider les collectivités à les utiliser, pour améliorer leur sécurité et accompagner des entreprises françaises. »

Centres de réponse régionaux : L'écosystème local doit également servir à répondre aux incidents, et l'identifier permet aux régions, devenues cheffes de file en matière de cybersécurité, de diriger correctement les victimes de cyberattaques. Ils ont bénéficié d'un accompagnement de l'Anssi à hauteur d'un million d'euros pour trois ans.

Un montant insuffisant, selon les agents de plusieurs régions engagées dans le parcours rencontrés dans les allées du FIC. Des solutions de financement sont à l'étude, que ce soit des formations payantes ou un accompagnement. L'enjeu étant de maintenir l'équilibre avec les offres proposées par des entreprises locales, sans les cannibaliser. Une autre option serait une prise en charge intégrale par la région, consacrant la valeur de service public d'une telle offre.

Outiller les collectivités : Une enquête menée auprès des plus petits collectivités montre que le prix est un des premiers freins à une protection efficace. C'est notamment pour cette raisons qu'un autre accompagnement a été imaginé par l'Anssi dans le cadre du plan de relance. L'appel à projet autour de la mutualisation a été lancé discrètement en mars et sera clos à la fin du mois de juin. L'objectif est de faciliter le déploiement de solutions de mutualisation des services les plus utilisés.

« On veut optimiser le déploiement et faire en sorte d'asseoir le rôle des mutualisants, c'est à dire les opérateurs publics de service numérique », explique Gwenaëlle Martinet. Plusieurs OPSN ont postulé et l'Adico a d'ores-et-déjà reçu une réponse positive pour quatre services.

La mutualisation des expériences peut se faire également par le biais des associations professionnels, notamment le Coter ou le Club de la sécurité numérique des collectivités (CSNC), qui tenaient également des stands à Lille. Le CSNC est né récemment et est toujours en cours de construction. Il vise à fédérer les RSSI pour qu'ils puissent partager leur veille, s'alerter ou agir de concert pour faire réparer des failles chez les éditeurs. Preuve en est, le « bug bounty » organisé par le Coter numérique et de trois collectivités, à la recherche des failles dans des logiciels utilisés par de nombreuses collectivités.

Une campagne pour sensibiliser les élus et agents : La plateforme Cybermalveillance.gouv.fr, qui accompagne les collectivités les plus petites dans leur sécurité informatique, a lancé une nouvelle campagne de sensibilisation. Inspirée par les fables de la Fontaine, elle décline les principales inquiétudes relevées par l'enquête menée auprès des plus petites collectivités.

Manque de sensibilisation, problème de moyens… Chaque a priori est évoqué par une fable. « Se libérer de ses préjugés, c'est assurer sa cybersécurité avant qu'il ne soit trop tard ! », rappelle la plateforme.

Antivirus, EDR ou XDR : Quelle est la différence?

De nos jours, aucun appareil n'est à l'abri d'une cyberattaque. Même ceux qui, autrefois, étaient et se disaient futés, à l'abri des attaques, présentent désormais des faiblesses à ne pas négliger.

En effet, tout appareil accédant à vos données doit être adéquatement protégé et ce, peu importe sa fonction (personnelle ou d'entreprise).

Il est important de bien comprendre qu'une attaque par rançongiciel n'arrive pas à l'exécution du chiffrement du poste. Au contraire, elle se prépare des semaines à l'avance, voire même des mois.

Quels sont les outils de prévention ?

1. L'Antivirus

L'antivirus est l'outil de protection le plus reconnu. D'ailleurs, il est celui sur lequel la confiance d'une majorité d'utilisateurs repose. L'antivirus aide à la prévention d'une attaque.

Il est construit à partir de deux modules précis : un engin et une bibliothèque de définition.

Tout d'abord, l'engin vérifie chaque fichier de votre appareil et il compare les codes de chacun d'entre eux avec ceux de la bibliothèque de signature. Ensuite, lorsqu'un fichier est identifié comme étant dangereux, il est placé en quarantaine et est isolé du système d'exploitation.

Finalement, si l'antivirus connait la méthode de nettoyage, il l'exécutera. Dans le cas contraire, il lancera une alerte afin que l'utilisateur puisse intervenir.

« À l'heure actuelle, le grand défi des entreprises en cybersécurité est la pénurie de main-d'œuvre, car elle limite la capacité d'analyser et de neutraliser les diverses attaques perpétrées. »

D'un exemple à l'autre

Vous souvenez-vous de la fameuse lettre d'amour, datant de la fin des années 1990?

Il s'agissait d'un scripte VBS caché derrière un simili fichier texte. Lorsque l'attaque avait été lancée pour la première fois, cette elle avait ravagée de nombreux postes et serveurs. À l'époque, ce virus était totalement inconnu des antivirus. Pour y remédier, le seul moyen était de déconnecter le réseau d'entreprise d'Internet, de télécharger la mise à jour du fichier de définition et de le déployer sur tous les postes.

De nos jours, la majorité des attaques sont de type *Zero-Day*, une attaque sans signature connue. Ces attaques sont très souvent basées sur une morphologie connue. En effet, de nombreux virus sont toujours en circulation, mais ont toutefois évolué selon les nouvelles tendances.

Endpoint Detection & Response (EDR)

Contrairement à l'antivirus, l'EDR effectue une analyse comportementale des menaces.

Il est considéré en tant qu'outil de surveillance en temps quasi réel. Il analyse l'exécution et il détermine s'il s'agit d'une menace. Toutefois, cette opération n'est pas basée sur une bibliothèque préalablement installée, mais plutôt sur l'incidence que le code aura sur *votre* appareil et ce, peu importe le type!

Qu'une attaque provienne d'une pièce-jointe d'un courriel, d'un ficher ou même d'un site Web, l'EDR sera en mesure de l'identifier.

Les cyberattaques installent des outils malveillants avant de passer à l'action. Pendant ce temps, l'EDR isole votre ordinateur le temps que le code soit neutralisé.

Extended Detection & Response (XDR)

Le XDR est l'extension de l'EDR. En effet, elle ajoute une corrélation entre les événements de sécurité en arrière-plan et l'intelligence artificielle afin de traiter les grands nombres de signaux. Le XDR se sert de l'infonuagique pour en optimiser l'analyse.

Dès lors, cet ajout améliore sa capacité à nettoyer et restaurer les dommages causés par un code malveillant. Cette capacité de guérison permet de rétablir l'appareil à son état initial.

La particularité d'un XDR est qu'il est fortement dépendant des services infonuagiques, en raison de la puissance de calcul et de traitement nécessaire pour analyser des trillions de signaux journaliers qui ne peuvent se restreindre à un seul appareil.

Un exemple frappant est celui de Microsoft, avec la suite *Defender*, qui traite, quotidiennement, jusqu'à 43 trillions de signaux. Très peu de compétiteurs peuvent avoir une vision approfondie de toutes les attaques ayant lieu à travers le monde. En effet, un algorithme d'apprentissage machine (*machine learning*) est en place pour capter tous les signaux. Il devient précis, jour après jour. Le premier but de l'apprentissage de machine est : le triage de l'information. En effet, le triage permet de cerner une attaque à travers une multitude d'information en constant mouvement.

Un dernier point

À l'heure actuelle, le grand défi des entreprises en cybersécurité est la pénurie de main-d'œuvre, car elle limite la capacité d'analyser et de neutraliser les diverses attaques perpétrées. Des données relevées au dernier recensement indiquent qu'il y a plus de 3.5 millions de postes à combler en cybersécurité à travers le monde.

En comparaison, vous pouvez installer le meilleur détecteur de fumée relié à une centrale, mais si vous ne disposez pas de la main d'œuvre pour analyser et pour intervenir, vous êtes toujours vulnérable à une attaque.

Il est donc impératif d'investir dans des outils fonctionnels et gérés par des spécialistes en cybersécurité. Grâce à l'intelligence artificielle, ces derniers seront en mesure d'analyser et de réagir adéquatement aux incidents.

Encore aujourd'hui, l'humain demeure au cœur de la solution.

Incendie d'OVH : une action collective lancée par sept entreprises

Suite à l'incendie du 10 mars 2021 qui a détruit une partie des datacenters d'OVHCloud à Strasbourg, une action en justice groupée a été initiée par plusieurs clients. Raison invoquée : le provider aurait manqué à ses obligations contractuelles.

[Mis à jour le lundi 15 novembre 2021 à 13h29] *Sept clients d'OVH qui ont vu leurs données partir en fumée dans l'incendie des data centers du groupe à Strasbourg le 10 mars dernier se sont regroupés pour lancer une action en justice commune (ou classaction). Ils sont représentés par Ziegler & Associés. "Etant tenu d'une responsabilité contractuelle de stockage et de sécurisation des données auprès de ses clients, OVHCloud a commis un manquement contractuel. Les entreprises touchées par cet incident ont droit à une indemnisation", explique maître Jocelyn Ziegler au JDN, avant de confier : "Une dizaine d'autres sociétés est en train d'évaluer l'intérêt qu'elles pourraient avoir à rejoindre la procédure." Qui sont ces entreprises ? Il s'agit principalement de PME qui n'ont pas les moyens de reconstituer les données perdues. Ayant souscrit à l'offre Hosted Private Cloud, toutes avaient leurs données hébergées dans le data center SBG1 détruit dans l'incendie. Problème : l'option de backup standard du service se contentait de répliquer les données dans le même centre de données, au sein d'une salle adjacente. "Dès que nous aurons regroupé 20 entreprises, nous enclencherons la procédure", confie Jocelyn Ziegler. "Cette action permettra d'être une force d'opposition, de réduire les frais de justice, et d'améliorer les chances d'obtenir une indemnisation."*

La feuille de route de cette class action ? Dans un premier temps, Ziegler & Associés entend évaluer le préjudice subi par chaque client ainsi que les dommages et intérêts correspondant. "Nous estimons que l'incendie n'est pas un cas de force majeur notamment dans la mesure où OVHCloud n'a pas tout mis en place pour y faire face. On peut évoquer par exemple l'absence de système d'extinction automatique dans le data center." Quant au préjudice, il s'évaluerait à l'aune des moyens nécessaires pour récupérer les données perdues, mais aussi en termes d'images pour les organisations touchées vis-à-vis de leurs propres clients et prospects. "Certaines d'entre elles ont été attaquées en justice par leurs clients pour avoir perdu leurs données", constate Jocelyn Ziegler. Parmi les PME impliquées

dans l'action groupée figurent des acteurs du tourisme, du SEA/SEO ou encore du médical. Des structures qui souhaitent rester anonymes pour éviter d'entacher plus largement leur image de marque. "Certains ont perdu des données de facturation ce qui leur pose des problèmes de paiement", reconnait Jocelyn Ziegler. "Pour d'autres, dans le domaine de la santé, il s'agit de données médicales de patients, notamment atteints de cancer." Des acteurs qui avaient pourtant activé l'option HDS (certification Hébergement de données de santé) de l'offre Hosted Private Cloud.

L'incendie qui a touché le campus d'OVH à Strasbourg le 10 mars 2021 a engendré un petit séisme sur le marché du data center. "Les appels d'offres des clients requièrent désormais des informations sur l'assurance de l'infrastructure, mais aussi des certifications APSAD (*qui concernent le mode de construction et de fonctionnement d'un bâtiment en termes de sécurité, ndlr*)", indique Arnaud de Bermingham, président de Scaleway, dans un podcast au JDN. Qu'en est-il des politiques des assureurs ? "Les primes de risque sont revues, voire même des clients résiliés. Les contrats seront conditionnés par des prérequis de certification complémentaires. Ce mouvement ne concerne pas uniquement la France", constate Arnaud de Bermingham.

Ces informations interviennent alors qu'un rapport d'expertise de Bureau Veritas sur la sécurité incendie du site de Roubaix, où l'opérateur héberge plus de 130 000 serveurs (contre 62 000 pour le site de Strasbourg), révèle les manques de la sécurité incendie de l'implantation historique. Comme à Strasbourg, le campus Roubaix n'est pas équipé de système automatique d'extinction (PJ N°4 de l'Etude d'impact) : "les installations ne sont pas équipées de RIA actifs, de systèmes de brouillard d'eau ou d'extinction automatique par sprinklage." Pas de mention d'extinction par gaz non plus (lire l'article Un rapport de Bureau Veritas révèle les manques de la sécurité incendie du site de Roubaix).

Suite à un premier incendie le 10 mars qui a détruit un des datacenters d'OVHCloud à Strasbourg et endommagé un second, un nouveau feu a pris vendredi 19 mars à 19h sur l'implantation. Il s'est déclaré au sein d'un conteneur hors tension du centre de données Strasbourg 1 (SBG 1), faisant office de local de stockage de batteries. 300 batteries de 25 kg ont été impactées. "Aucun blessé n'est à déplorer parmi les équipes d'OVHcloud ou de ses partenaires. Deux personnes de la sécurité ayant été incommodées par les fumées ont été examinées par des professionnels de santé", précise le groupe. L'incendie a été rapidement maitrisé par les pompiers. Mobilisant 130 personnes, les opérations visant à remettre les infrastructures en production suite au premier incendie ont été interrompues pour la nuit. L'alimentation de SBG 1 dont les serveurs étaient en cours de redémarrage, a été coupée par mesures de précaution. Dans la foulée, OVHCloud a annoncé que tous les serveurs SBG 1 seraient finalement déplacés sur d'autres datacenters situés sur le site de Strasbourg, ou sur ses campus de Gravelines et Roubaix, avec un passage par son usine de Croix pour être dépollués suite au dégagement de fumée. Une décision qui a semble-t-il été prise en lien avec son assureur. L'origine de ce second incident est toujours indéterminée.

Photo de l'incendie du site d'OVH à Strasbourg le 10 mars au matin.
© Service d'incendie et de secours du Bas-Rhin

OVH avait commencé dans la nuit du 17 mars à rebooter progressivement les machines encore fonctionnelles sur Strasbourg 3 et 4 après vérification de l'état de chacune. Le 22 mars, la Cnil a publié sur son site web une note le lundi 22 mars. Son titre est sans équivoque : "Incendie OVH : faut-il notifier à la CNIL ?" . Dans ce document, la commission rappelle qu'une notification est nécessaire "si des données personnelles ont été définitivement perdues ou si elles sont restées indisponibles suffisamment longtemps, de telle sorte que cela a engendré un risque pour les personnes." Elle ajoute : "Si la violation est susceptible d'engendrer des risques élevés pour les personnes, celles-ci doivent également être directement informées par le responsable de traitement."

Six mois offerts en cas de perte de données

Le 22 mars dans l'après-midi, Octave Klaba a posté une troisième vidéo sur Twitter pour faire le point sur la situation. Concernant l'enquête en cours sur l'incendie, le CEO insiste sur le nombre d'intervenants : police judiciaire, BEA, assureurs, experts indépendants, huissiers... "Cette enquête va prendre plusieurs mois. Nous en partagerons évidemment toutes les conclusions", insiste le PDG. Mais Octave Klaba entend tirer les enseignements du sinistre sans attendre. "Nous avons décidé de créer un laboratoire pour travailler sur les différents cas de départ de feu au sein d'un datacenter, sur la capacité des portes et cloisons à maintenir le feu, et sur les méthodes d'extinction les plus efficaces selon les cas de figure. Nous comptons publier ces méthodes en open source pour en faire bénéficier le maximum d'entreprises".

Dans une vidéo précédente diffusée le 16 mars, Octave Klaba avait indiqué que les clients bénéficieraient de trois mois gratuits en cas d'une coupure de service et de six mois gratuit en cas de perte de données.

L'offre Private Cloud touchée en plein cœur

Le groupe a dressé un état des lieux des sauvegardes de données non-récupérables ou en cours d'investigation en fonction du centre de données utilisé et du service souscrit. Une information cruciale pour permettre à ses clients de restaurer leur site web et autres applications cloud sans attendre. Principale surprise : au sein de SBG1, l'offre de cloud privé d'OVH (Private Cloud) était hébergée dans

une salle, et son backup dans une autre salle du même datacenter. Les deux ont été détruites dans l'incendie. A moins d'avoir pris la précaution de mettre en œuvre un second backup chez un autre provider, les données sont donc perdues.

Rappelons que la solution Private Cloud est historiquement positionnée sur le haut de gamme. Par ailleurs, 20% des sauvegardes des VPS/PCI basés sur l'infrastructure alsacienne d'OVH sont aussi parties en fumée. Les clients dont les backups font partie de ses 20% n'ont plus qu'à espérer que leur(s) serveur(s) privé(s) virtuel(s) ont été épargnés.

De nombreux backups irrécupérables

La facturation a par ailleurs été suspendue à la date de l'incendie pour tous les clients utilisant les services sur les les datacentres d'OVH à Strasbourg. En attendant leur remise en service, des infrastructures alternatives leur on été proposées gratuitement (serveur bare metal, Hosted Private Cloud et Public Cloud) sur les centres de données du groupe à Roubaix et Gravelines. OVH a par ailleurs mis en ligne un questions-réponses à destination de ses clients pour leur permettre de faire face à la situation.

Le feu aurait pris dans un onduleur

Le PDG du groupe, Octave Klaba, a pris la parole une première fois sur Twitter le 11 mars. Une vidéo de 8 minutes dans laquelle il revient sur les circonstances de l'événement. Le CEO présente ses excuses aux clients et promet qu'un tel événement ne se reproduira pas. Voici ce qu'il faut retenir :

- L'incendie a pris dans le datacenter SBG2 qui a été entièrement détruit. Les alertes incendie ont bien fonctionnées. Mais le feu s'est répandu trop rapidement pour permettre aux agents sur site d'intervenir.
- OVH met à disposition des clients impactés des ressources alternatives (serveurs dédiés, Public Cloud, Private Cloud) dans ses datacenters de Roubaix et de Gravelline.
- Le rythme de fabrication dans l'usine d'OVHCloud à Croix passe à 2500-3000 serveurs par jour pour répondre à la demande.
- Les caméras thermiques des pompiers arrivés sur place 15mn après la première alerte ont détecté deux onduleurs en feu au sein de SBG2, dont l'un avait fait l'objet d'interventions le jour même dans la matinée avant d'avoir été remis en service dans l'après-midi.
- SBG2 repose sur une technologie qui remonte à 2011. Il s'agit d'une tour autoventilée qui fonctionne par la différence de pression entre le haut et le bas de l'édifice. De génération 2016, SBG3 repose sur une technologie qui a évité son embrasement.
- OVH compte utiliser les vidéos des 300 caméras de surveillance de son site de Strasbourg pour retracer l'historique de l'incendie, comprendre précisément ce qui s'est passé en vue d'en tirer tous les enseignements.

Un déflagration pour la French Tech

Suite à l'incendie qui s'est déclaré dans la nuit du 9 au 10 mars sur le site d'OVHCloud à Strasbourg, 3,6 millions de serveurs HTTP représentant 464 000 noms de domaines se sont retrouvés hors ligne. Le chiffre est publié par Netcraft, spécialiste américain du monitoring d'Internet. "Plus de 18% des adresses IP attribuées à OVH dans notre dernière Web Server Survey publiée il y a deux semaines ne répondaient plus le 10 mars entre 7h et 8h du matin", indique Netcraft. De son côté, Downdetector recensait au même moment plusieurs centaines de rapports d'erreur. OVHCloud évoque quant à lui 12 000 à 16 000 clients touchés. Alors que les GAFAM pénètrent l'Europe avec une force

concurrentielle sans merci, c'est une véritable déflagration pour la French Tech dont l'image va de facto se ternir. Son porte-flambeau a subi la plus importante catastrophe industrielle de son histoire.

Le datacenter Strasbourg 2 (SBG2) du cloud français a été entièrement ravagé par les flammes. Du côté du SBG1, quatre salles serveurs ont été détruites. Huit ont échappé à l'incendie, ainsi que les salles réseau. Les serveurs de SBG3 n'ont pas non plus été touchés.

Un communiqué de presse a été diffusé par l'entreprise dans les heures suivant la déclaration de l'incendie : "Ce mercredi 10 mars 2021, à 00h47, un incendie s'est déclaré dans une salle d'un de nos quatre datacentres strasbourgeois, SBG2. Nous précisons que le site ne fait pas l'objet d'une classification Seveso. Les pompiers sont immédiatement intervenus sur site afin de protéger les équipes et limiter la progression de l'incendie. Ils ont ainsi procédé à l'isolation complète du site et de son périmètre dès 2h54. À 4h09, le feu a détruit SBG2 et continuait de présenter des risques pour les datacentres voisins jusqu'à ce que les pompiers prennent le contrôle complet de l'incendie." Le PDG d'OVHCloud a immédiatement recommandé à tous ses clients d'activer le "Disaster Recovery Plan".

115 pompiers mobilisés

L'implantation d'OVHCloud à Strasbourg est situé sur un ancien site du sidérurgiste ArcelorMittal dans le quartier du Port du Rhin. Mobilisant 115 pompiers, 43 véhicules, six lances-canons et deux échelles, l'incendie a finalement été circonscrit aux alentours de 5h30 du matin le 10 mars. "Des moyens opérationnels ont également été mobilisés par les autorités allemandes", souligne la préfecture du Bas-Rhin dans un communiqué. Les quelques collaborateurs présents sur site ont rapidement été pris en charge par les pompiers.

Aux côtés de SBG2 qui a été entièrement détruit, le datacenter SBG1 aura donc été largement touché. "Les pompiers ont pu protéger SBG3. Pas d'impact sur SBG4.

SBG2, le datacenter où le feu s'est déclaré, compte cinq étages et s'étend sur un total de 1900 m2. Les flammes sont montées à plusieurs dizaines de mètres. Inauguré en 2012, il possède une capacité de 14 000 serveurs. Il abrite une partie de la très stratégique offre Hosted Private Cloud ciblant les grands clients d'OVHCloud. Cette solution d'IaaS basée sur la technologie de virtualisation de VMware est entièrement infogérée par les équipes du groupe. SBG2 héberge également des serveurs dédiés utilisés par de nombreux sites web français.

S'exprimant sur Twitter, certains clients ayant omis de faire une sauvegarde de leurs données se sont retrouvé en grande difficulté. C'est le cas du jeu Rust, ou encore du cabinet d'huissiers Leroi & Associés qui a indiqué avoir perdu ses mails suite à l'incendie. A l'image de ce cabinet, de nombreux utilisateurs issus de presque toutes les régions de France s'inquiétaient le 10 mars sur le forum de Downdetector de l'impossibilité d'accéder à leur messagerie chez OVH. Le service de Mail du groupe a été remis en service le 11 mars à 1h22 du matin.

Des conséquences qui démontrent l'importance de souscrire à un service de sauvegarde sur un datacenter situé sur une autre géographie, voire chez un autre provider pour pallier les pannes qui pourraient affecter tous les centres de données du fournisseur, tel un crash réseau se répercutant par richochet à tous les services.

Un plan de reprise d'activité a été immédiatement déployé. Au programme : la remise en service de l'alimentation électrique du datacenter SBG3 (de 20 KV), mais aussi celles de SBG4 (de 240 KV). Une salle réseau temporaire a été mis en place pour le SBG5. Enfin, le raccordement en fibre optique aux

datacenters d'OVHCloud de Paris et Frankfurt a d'ores et déjà été contrôlé et n'a pas été touché par l'incendie.

De multiples sites web touchés

On a relevé évidemment de nombreux sites touchés : data gouv (qui a depuis été remis en ligne), les sites d'Esri France, du Centre Pompidou à Paris, du CREPS Rhône-Alpes, de la Fédération des Médecins de France, de Génération 5, du Kiosque So Press, de l'Office de tourisme de Colmar...

Nos confrères des DNA ont également recensés les sites suivants : ceux de l'aéroport de Strasbourg, de l'ENT (espace numérique de travail) ONE & NEO à Sarreguemines, de la ville de Cherbourg, du comité d'entreprise de Peugeot-Sochaux, de la brasserie Meteor, du site de réservation de scooters électriques Cityscoot (en région parisienne), de la ville de Vichy, du club de rugby de Clermont-Ferrand, du site de l'UPR (le parti politique de François Asselineau), du stade de Caen, de l'office de tourisme de Saverne, celui de Recyclivre, de l'université populaire européenne. A noter que des sites allemands, italiens, espagnols, polonais ou turcs sont aussi touchés par la panne.

BFM a évoqué de son côté les sites et services suivants : ceux des villes d'Arras ou de Saint-Ouen, plusieurs médias, dont Le Nouveau détective et Front populaire, le média lancé par Michel Onfray. Le site Internet de la chaîne a également cité des clubs sportifs, dont l'ASM Rugby, l'US Créteil Handball ou encore l'AS Saint-Priest.

Un système anti-incendie peu efficace

Reste à savoir si le système anti-incendie déployé dans les datacenters d'OVH à Strasbourg a bien fonctionné. Un dispositif de détection des feux y est bien installé, et des exercices anti-incendie y sont réalisés tous les 6 mois. Mais les premières flammes qui se sont déclarées au sein du datacenter SBG2 ont-elles été identifiées par ce système ? Les procédures prévues ont-elles été correctement mises en œuvre ? Au-delà de ces questions, une certitude demeure : Les centres de données d'OVHCloud à Strasbourg ne sont pas dotés de réseaux d'extinction. Ils ne sont pas équipés de gicleurs d'eau comme c'est le cas dans les datacenters d'OVHCloud à Beauharnois au Canada, ni de brumisateurs haute pression permettant de résorber les flammes tout en protégeant les machines contre l'eau, ni de gaz inerte, à l'instar de la plupart des datacenters du marché. Des gaz qui ont pour vocation de vider les salles serveurs de leur oxygène pour étouffer l'incendie en évitant là-encore de causer des dégâts aux équipements.

Le vendredi 26 mars, l'intégralité du data center SBG4 était de nouveau fonctionnelle, ce qui n'était pas encore le cas de SBG3.

L'information intervient alors qu'OVHCloud a annoncé ce 9 mars son intention d'entrée en bourse. Octave Klaba et sa famille entendent néanmoins conserver la majorité des actions suite à l'opération.