HORS SERIE

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

CYBERSÉCURITÉ & TERRITOIRES

THEGREENBOW

Ce numéro de GlobalSecurity Mag vous est offert par THEGREENBOW

Hors série N°018 - Prix : 7 € - juin 2017

USERCUBE

GOUVERNANCE et ADMINISTRATION des IDENTITÉS

SOLUTION DE NOUVELLE GÉNÉRATION

ON PREMISE & AZURE

- Cycle de vie des Identités
- Gestion des règles et des rôles
- Role Modeling / Role Mining
- Workflow d'administration (demande et validation)
- Recertification des accès
- Contrôles de sécurité automatisés
- Audit, traçabilité et reporting
- Provisioning automatique et ouverture de tickets
- Self-service de mot de passe

www.usercube.com | contact@usercube.com | 09 72 31 03 15

ÉDITORIAL
DE MARC JACOB

PAS DE CONNEXION INTERNET, PAS DE DÉVELOPPEMENT ÉCONOMIQUE !

Les élus des collectivités territoriales ont compris que le développement de leur région passe désormais par l'avènement du numérique et des réseaux télécom. Le haut débit est aujourd'hui devenu aussi indispensable que l'eau ou l'électricité. En effet, aucune entreprise ne peut survivre sans une bonne connexion Internet, car toutes les démarches administratives, les relations avec la banque, les clients… passent par le Web. Pourtant, nous sommes loin d'avoir une couverture homogène sur l'ensemble du territoire. Dans certaines villes, comme à Plestin les Grèves en Bretagne, les citoyens ont le choix entre se connecter à Internet ou regarder la télé… D'un côté, ils peuvent se consoler en se disant que ce manque de connectivité limite leur risque de cyberattaque…

Comment obtenir cette connexion alors que la libre concurrence dans les télécoms incite les opérateurs à ne couvrir que les zones rentables ? Certains prônent les partenariats public-privé, mais pour autant il faut qu'ils restent rentables pour le privé. D'autres souhaitent le soutien actif de l'État, mais c'est immanquablement s'opposer aux décisions de l'Europe en ce domaine.

Dans ce nouveau contexte, comment désenclaver les territoires, ramener les habitants dans les petits villages et drainer un tissu économique ? Certains élus locaux essaient de développer des Data Centers qui attirent des entreprises et, par conséquent, des habitants amorçant ainsi la pompe d'un cercle vertueux… D'autres essaient de se servir des atouts de leurs régions : tourisme, spécialités régionales… mais peu sont ceux qui réussissent ce pari. Les collectivités territoriales sont donc prises aujourd'hui au piège. Il faudra des décisions radicales pour les en sortir !

REVUE TRIMESTRIELLE
Hors Série n°18 – Juin 2017
www.globalsecuritymag.fr et www.globalsecuritymag.com
ISSN : 1961 – 795X
Dépôt légal : à parution
Editée par SIMP
RCS Nanterre 339 849 648
17 avenue Marcelin Berthelot
92320 Châtillon
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : marc.jacob@globalsecuritymag.com

RÉDACTION
Directeur de la Publication :
Marc Brami
Rédacteur en chef :
Marc Jacob
Rédactrice :
Emmanuelle Lamandé
Ont collaboré à ce numéro :
Yves Jussot, Bénédicte Pilliet et Jean-Paul Mazoyer
Assistante :
Sylvie Levy
Responsable technique :
Raquel Ouakil
Photos
Marc Jacob
Comité scientifique :
Pierre Bagot, Francis Bruckmann Eric Doyen, Catherine Gabay, François Guillot, Olivier Iteanu, Dominique Jouniot, Patrick Langrand, Yves Maquet, Thierry Ramard, Hervé Schauer, Michel Van Den Berghe, Bruno Kerouanton, Loïc Guézo et Valentin Jangwa
In Memoriam, notre regretté Zbigniew Kostur

PUBLICITE
S.I.M Publicité
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : ipsimp@free.fr

PAO
S.I.M. Publicité
Image couverture : ©tai11, Anton Balazh

IMPRESSION
Imprimerie Moutot
33-37 Rue Hippolyte Mulin
92120 Montrouge
Tél. 01 46 57 79 79
e-mail : contact@imprimeriemoutot.fr

ABONNEMENT
Prix de ce numéro :
7 € TTC (TVA 20%)
Abonnement annuel :
51 € TTC (TVA 20%)

Sécurisez les accès des personnes en mobilité

THEGREENBOW

Unique solution VPN pour des connexions sécurisées agréées

TheGreenBow VPN
Certifié CC EAL3+,
Qualifié standard,
agréé DR OTAN/UE

disponible pour tout équipement

Windows Linux MAC Android iOS

Logiciel VPN universel de confiance : connexion sécurisée avec toute passerelle VPN IPsec ou SSL, opérationnel sur réseau WiFi, 3G, ADSL et satellite, compatible toute IGC/PKI, compatible tout support d'authentification, token, carte à puce et OTP, Certifié CC EAL3+, Qualifié niveau standard, Agréé Diffusion Restreint OTAN et Union Européenne, habilité pour tous OIV.

www.thegreenbow.com

Sommaire

Guide des solutions

Agenda

JUILLET

4 - 7 juillet - Singapour
INTERPOL World
www.interpol-world.com

5 juillet - Londres (UK)
PCI London
www.pci-portal.com/events

6 - 7 juillet - Fleurance
Cybersécurité & Territoires
http://cybercercle.com

12 juillet - Paris
Matinale du CyberCercle
www.cybercercle.com

18 - 20 juillet - Nairobi (Kenya)
SecProTec East Africa
www.secproteceastafrica.com

22 - 27 juillet - Las Vegas (USA)
Black Hat Training & Briefings USA
www.blackhat.com

26 - 28 juillet - Washington, D.C. (USA)
Biometrics for Government and
Law Enforcement International Summit
https://biometricsinternationalsummit.iqpc.com

26 - 28 juillet - Sydney (Australie)
Security Expo
www.securityexpo.com.au

27 - 30 juillet - Las Vegas (USA)
DEFCON
www.defcon.org

AOÛT

6 - 9 août - Austin (USA)
DFRWS USA
www.dfrws.org/conferences/dfrws-usa-2017

16 - 18 août - Ile Maurice
Audit Risk & Governance Africa
Cyber Crime Africa Summit
www.auditriskgovernanceafrica.misti.com

SEPTEMBRE

5 - 6 septembre - Singapour
DiCyFor Security Summit
www.dicyfor.com

5 - 7 septembre - Bucarest (Roumanie)
Cyber Intelligence Europe
www.intelligence-sec.com/events/cyber-intelligence-europe-2017

6 - 8 septembre - Las Vegas (USA)
InterDrone
www.interdrone.com

7 septembre - Paris
Université d'Eté d'HEXATRUST
www.hexatrust.com

14 - 17 Septembre - Istanbul (Turquie)
ISAF
www.isaffuari.com/en

20 septembre - Paris
Security Tuesday - ISSA France
www.securitytuesday.com

25 septembre - Paris
Trophées de la sécurité
http://tropheesdelasecurite.fr

25 - 27 septembre - Marseille
Smart Security Week
www.smartsecurityweek.com

26 - 28 septembre - Porte de Versailles - Paris
Salons Solutions
www.salons-solutions.com

26 - 28 septembre - Porte de Versailles - Paris
APS
www.salon-aps.com

27 septembre - Paris
Matinale du CyberCercle
www.cybercercle.com

27 - 28 septembre - Londres (UK)
Cyber Security for Critical Assets Europe
www.cs4ca.com/europe

OCTOBRE

2 - 5 octobre - Toronto (Canada)
MAAWG
www.m3aawg.org

3 - 4 octobre - Dakar (Sénégal)
Préventica
www.preventica-africa.com

3 - 4 octobre - Paris - Porte Maillot
Microsoft expériences
https://experiences.microsoft.fr

4 - 6 octobre - Madrid (Espagne)
Virus Bulletin
www.virusbulletin.com/conference/vb2017

8 - 12 octobre - Dubaï (EAU)
GITEX Technology Week
www.gitex.com

10 - 12 octobre - Nuremberg (Allemagne)
it-sa
www.it-sa.de

11 - 14 octobre - Monaco
Les Assises de la Sécurité
www.les-assises-de-la-securite.com

Par Yves Jussot, référent ANSSI pour la région Occitanie

SÉCURITÉ NUMÉRIQUE ET TERRITOIRES : NOUS AVONS TOUS UN RÔLE À JOUER

Que l'on soit un acteur privé ou public, local ou national, de grande ou de petite taille, issu de tel ou tel secteur d'activité, nous sommes tous concernés par les défis que représente le développement du numérique. Vecteur de croissance et d'innovation, il peut aussi devenir une faiblesse en créant de nouvelles failles et vulnérabilités. C'est pourquoi il doit également s'accompagner d'une réelle prise en compte des enjeux de la sécurité, et ce à tous les niveaux. Susciter cette prise de conscience, c'est le défi que relève au quotidien l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, dans le cadre de ses missions de prévention, de défense et de sensibilisation des acteurs-clés de la société du numérique.

Qu'il s'agisse d'ordinateurs, de tablettes, d'objets connectés, de réseaux informatiques ou de télécommunications, toutes ces nouvelles technologies dont nous sommes de plus en plus dépendants envahissent notre société, notre économie et l'ensemble de nos activités. Cette dépendance comporte des risques accrus qui doivent être appréhendés : cybercriminalité, espionnage, atteinte à l'image, voire sabotage, sont autant de menaces qui peuvent affecter les collectivités locales, les petites et grandes entreprises ou encore les administrations centrales.

Un constat s'impose : nous sommes tous vulnérables, chacun détenant des données potentiellement intéressantes, suscitant la convoitise d'acteurs malveillants. L'un des enjeux aujourd'hui est avant tout d'assurer une prise de conscience de l'ensemble des acteurs économiques et politiques face à ces risques, et ce au « bon » niveau, afin de pouvoir ensuite mettre en place des actions efficaces de prévention et de réaction pour mettre en échec l'essentiel des attaques potentielles.

Tous vulnérables, mais aussi tous acteurs de la sécurité du numérique. Il existe, en effet, tout un ensemble de réponses à la fois techniques, organisationnelles et méthodologiques à la portée de tous. Certains acteurs, publics ou privés, de taille et de budget plus modestes ne disposent pas de personnes consacrées spécifiquement à la protection des systèmes d'information. Il est nécessaire de leur apporter des solutions concrètes et abordables.

Les référents territoriaux de l'ANSSI en charge de la sécurité numérique ont aussi pour mission de sensibiliser les acteurs locaux, des TPE/PME aux collectivités territoriales, et de les accompagner à entreprendre une démarche visant à développer la sécurité de leurs systèmes d'information. C'est pour cela que le référent de l'ANSSI va, par exemple, chercher à toucher des associations d'entreprises pour générer un partage des expériences positives et ainsi créer une véritable dynamique commune qui bénéficiera à la compétitivité de l'ensemble des entreprises de la région.

Le rôle de l'ANSSI est aussi d'éclairer l'offre de services privée en proposant sur son site Internet des listes de prestataires de qualité et de confiance, adaptés aux différents publics. Il existe tout un ensemble de produits de sécurité - des pare-feux aux outils de chiffrement - dont un certain nombre ont été labellisés par nos services. Cela signifie que nous en avons testé l'efficacité et que nous avons confiance dans les éditeurs concernés. Autre exemple, le *cloud* permet à une petite structure de confier à un prestataire l'hébergement et le traitement de ses données dans un datacenter avec une sécurité physique, des sauvegardes, des services bien configurés et des mises à jour. Cette externalisation peut constituer une solution intéressante à condition de bien l'encadrer, d'où l'élaboration de guides à destination des non-initiés à la sécurité informatique pour accompagner leurs choix (points d'attention à ne pas manquer, clauses contractuelles types).

Plus récemment, l'agence a participé à la création du dispositif national d'assistance aux victimes d'actes de cybermalveillance, aux côtés du ministère de l'Intérieur. La plateforme « cybermalveillance.gouv.fr », actuellement en phase d'expérimentation dans la région Hauts-de-France, a notamment pour mission de mettre en lien des victimes, particuliers ou acteurs publics et privés, avec des prestataires de proximité susceptibles de les assister techniquement.

Enfin, une prévention efficace commence encore et toujours par la mise en place de bonnes pratiques qui relèvent souvent du bon sens : mise à jour régulière des logiciels, choix de mots de passe robustes, mise en place d'un système de sauvegarde ou encore séparation des usages à caractère personnel de ceux à caractère professionnel. Ces mesures très simples sont répertoriées dans l'ensemble des guides publiés par l'ANSSI (bonnes pratiques, hygiène informatique), ainsi que dans les notes techniques. L'ensemble de cette documentation est accessible gratuitement sur notre site Internet : www.ssi.gouv.fr. ■■■

Interview d'Alice de La Mure, Juriste au service CIL (Correspondants informatique et libertés) de la CNIL
Par Marc Jacob et Emmanuelle Lamandé

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

DPO MUTUALISÉ : UNE BONNE ALTERNATIVE POUR LES COLLECTIVITÉS TERRITORIALES

Les collectivités territoriales traitent chaque jour de nombreuses données sensibles dans le cadre de leurs missions et sont, de ce fait, soumises à de multiples règlementations en matière de protection et de conservation des données : loi Informatique & Libertés, loi « Archives », loi CADA... Elles auront, de plus, l'obligation de désigner un *Data Privacy Officer* d'ici mai 2018, dans le cadre de la mise en application du RGPD. Alice de La Mure leur recommande d'ailleurs de ne pas attendre cette échéance et de nommer dès à présent un CIL ou du moins de déterminer qui pourrait occuper cette fonction. La mutualisation s'avère également, selon elle, une bonne alternative pour les structures n'ayant pas les ressources nécessaires en interne.

Global Security Mag : Les collectivités territoriales traitent chaque jour de nombreuses données personnelles dans le cadre de leurs missions. Quels sont les enjeux inhérents à ces traitements ?

Alice de La Mure : Effectivement, les collectivités territoriales traitent chaque jour de nombreuses données personnelles, que ce soit pour assurer le fonctionnement de leur structure (fichiers RH par exemple), la sécurisation de leurs locaux (contrôle d'accès par badge, vidéosurveillance...) ou, bien entendu, la gestion des différents services publics et activités dont elles ont la charge. Certains de leurs traitements présentent une sensibilité particulière, comme les fichiers d'aide sociale et ceux de la police municipale. L'article 1er de la loi Informatique & Libertés du 6 janvier 1978 modifiée fixe ainsi comme principe directeur que « l'informatique doit être au service de chaque citoyen », qu' « elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Aujourd'hui, les enjeux pour les collectivités territoriales sont de taille. En effet, l'e-administration constituant un levier majeur de la modernisation de l'action publique, ces dernières recourent de plus en plus aux nouvelles technologies et usages informatiques : téléservices, open data, systèmes d'information géographique, cloud computing, compteurs intelligents, réseaux sociaux, lecture automatique de plaques d'immatriculation... Dans le même temps, le nombre de cyberattaques ne cesse d'augmenter, et ce, quelle que soit la taille des organisations visées. En outre, le niveau de conscience des citoyens quant au besoin de protection de leurs données est de plus en plus important, tandis que la loi pour une République numérique est venue consacrer en octobre 2016 un droit à l'auto-détermination informationnelle que l'on retrouve posé à l'article 1er de la loi Informatique et Libertés : « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant ». Enfin, à la veille de la mise en application du RGPD (Règlement général européen relatif à la protection des données personnelles), qui s'articule autour d'une logique nouvelle de responsabilisation de l'ensemble des organismes traitant des données personnelles, et renforce encore les droits des personnes concernées ainsi que le pouvoir répressif des autorités de contrôle, les acteurs publics doivent nécessairement se mettre en ordre de marche.

LES COLLECTIVITÉS TERRITORIALES DOIVENT COMBINER LES OBLIGATIONS DE LA LOI INFORMATIQUE & LIBERTÉS...

GS Mag : Quelles sont les différentes obligations qui incombent aujourd'hui aux collectivités territoriales en matière de sécurité et de protection des données ?

Alice de La Mure : Les collectivités territoriales doivent tenir compte, au même titre que toutes les entreprises, des 5 règles d'or imposées par la loi Informatique & Libertés de 1978 :

- Le principe de finalité des traitements, en vertu duquel les données sont collectées pour un but bien déterminé et légitime, et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial. Ce principe limite la manière dont le responsable de traitement pourra utiliser ou réutiliser ces données dans le futur. Un maire, par exemple, ne pourra pas se servir du fichier des inscriptions scolaires pour faire de la communication politique. La liste électorale pourra en revanche être utilisée à un telle fin.
- Le principe de pertinence et de proportionnalité des données collectées : seules les données strictement nécessaires à la satisfaction de l'objectif poursuivi doivent être collectées. A titre d'exemple, seule la mention « Personne en fauteuil roulant » devra être enregistrée si la précision du handicap ou de la maladie en cause n'est pas nécessaire pour assurer une prise en charge adéquate de l'intéressé. Il s'agit donc de minimiser autant que possible la collecte des données.
- Le principe de durée limitée de conservation des données collectées : ces données ne doivent être conservées sous une forme identifiante et en « base active » que le temps nécessaire à la réalisation de l'objectif poursuivi (par exemple, tant que l'administré bénéficie d'une prestation publique) et doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques...
- Le principe de sécurité des données : le responsable de traitement doit prendre toutes les mesures utiles pour garantir l'intégrité et la confidentialité de ces données, en s'assurant notamment que des tiers non autorisés n'y auront accès. Ces mesures seront déterminées en fonction des risques (sensibilité des données, objectif du traitement...) et seront à la fois d'ordre physique, logique, technique et organisationnel (sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques, encadrement des opérations sous-traitées...).
- Le principe du respect des droits des personnes : les personnes concernées par les traitements doivent conserver la maîtrise des données qui leur sont relatives. Ainsi, la loi prévoit que les données ne peuvent être collectées à l'insu des personnes concernées, qui doivent avoir été informées au préalable de cette opération, de sa finalité, des destinataires des données et des modalités d'exercice de leurs droits. Ces droits « Informatique et Libertés », qu'elles peuvent exercer auprès de l'organisme qui détient ces informations, sont principalement : le droit d'accéder à leurs données et d'en obtenir une copie, le droit de les rectifier en tant que de besoin et le droit de s'opposer à leur utilisation, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). La loi pour une République numérique d'octobre 2016 est venue renforcer ces droits en prévoyant notamment la possibilité pour les personnes concernées de les exercer par voie électronique, ainsi que de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.

Le respect de ces 5 règles d'or, dont la pertinence n'a jamais été démentie et que l'on retrouve ainsi quasiment à l'identique dans le RGPD, garantit l'effectivité de la protection apportée aux données personnelles traitées. Leur prise en compte par les décideurs publics constitue un gage de sécurité juridique, en les protégeant notamment contre un risque pénal particulièrement important, un gage de sécurité informatique profitable à l'ensemble du patrimoine informationnel de la collectivité, ainsi qu'un vecteur de confiance et de valorisation de l'image de cette dernière auprès de toutes les personnes concernées par ses traitements (employés et administrés en particulier). Ainsi, si la conformité a un coût, elle doit surtout être perçue comme un investissement.

... AVEC CELLES DE LA LOI « ARCHIVES »...

GS Mag : Quid concernant la conservation de ces données et leur communication à des tiers ?

Alice de La Mure : En matière de conservation des données collectées, les collectivités territoriales doivent combiner les obligations de la loi Informatique & Libertés, et en particulier la règle de durée limitée de conservation des données tel qu'évoqué précédemment, avec celles de la loi « Archives » de 1979 dont on retrouve les dispositions dans le Code du Patrimoine et qui impose parfois, à des fins historiques statistiques ou scientifiques, un archivage de celles-ci ad vitam aeternam. Ces deux régimes juridiques protègent des intérêts aussi différents que complémentaires dans une société démocratique : d'un côté, le droit à la vie privée et à « l'oubli » de l'individu, de l'autre, le droit à la mémoire de la société.

Schématiquement, deux ou trois phases caractérisent le cycle de vie des données contenues dans les documents/fichiers détenus par les organismes chargés de missions de service public :

- La conservation des données en « base active », tout le temps de leur utilisation courante par le service opérationnel concerné ;
- Puis, l'archivage intermédiaire des données ne présentant plus qu'un intérêt administratif (faire valoir des droits, évaluer une activité), sur une base dite « intermédiaire » accessible aux seules personnes habilitées à en connaître, pour gérer notamment un éventuel contentieux (un isolement des données au moyen d'une séparation logique – restriction des droits informatiques permettant l'accès aux données – peut suffire) ;
- Enfin, à l'issue de la « durée d'utilité administrative » et dans certains cas, l'archivage définitif des données dont l'intérêt historique, statistique ou scientifique justifie qu'elles ne fassent l'objet d'aucune destruction et qu'elles soient conservées et valorisées par le service d'archives publiques compétent (par exemple, les registres de l'état civil).

Le service interministériel des Archives de France (SIAF) et son réseau d'archives départementales ont compétence, dans le cadre du contrôle scientifique et technique de l'État défini par le Code du patrimoine, pour déterminer le cycle de vie des archives publiques. Pour s'orienter dans le pilotage des

mobility for business

Solutions mobiles pour une meilleure transformation digitale des entreprises

17 & 18 OCTOBRE 2017

PARIS - PORTE DE VERSAILLES

Platinum Sponsor

praxedo
Solution Cloud de gestion d'interventions

Gold Sponsors

izOrder

redhat.

en partenariat avec

L'INFORMATICIEN

www.mobility-for-business.com

différentes phases, les collectivités devront ainsi s'appuyer sur les délibérations de la CNIL concernant leurs traitements de données personnelles, ainsi que sur les circulaires/instructions/tableaux de gestion, de tri et de conservation des archives émanant des autorités compétentes. Afin de répondre au mieux à l'ensemble des exigences, il est également essentiel que les personnes veillant à la protection des données personnelles travaillent de concert avec les services opérationnels, juristes, informaticiens et archivistes sur cette question de la durée de conservation des données.

Concernant la communication des données personnelles à des tiers, la loi Informatique et Libertés impose donc aux collectivités territoriales de veiller à ce que ces données ne soient pas transmises à des personnes non autorisées à en connaître. De telles transmissions vont ainsi pouvoir intervenir que dans le respect de certaines conditions. D'une part, dans le cadre de contrats de prestation de service, qui indiqueront expressément que le sous-traitant ne pourra intervenir sur les données que sur instruction et sous la responsabilité de la collectivité donneur d'ordres, ainsi que dans des conditions de nature à garantir la sécurité des informations traitées. D'autre part, dans le cadre de partenariats institutionnels, inter-administrations notamment, et sous réserve que ces communications de données se fassent en toute transparence vis-à-vis de la CNIL (partenaire identifié comme un destinataire des données dans le dossier de formalités préalables) et des personnes concernées qui devront avoir été mises en mesure de s'y opposer. Ces dernières ne pourront cependant pas refuser cette communication d'informations si celle-ci répond à une obligation légale, quand bien même la réutilisation des données servirait un objectif incompatible avec celui ayant présidé à leur collecte. Il en va ainsi (par exemple, des communications de données sur demande de l'administration fiscale ou d'officiers de police judiciaire agissant dans le cadre des prérogatives que leur reconnaissent respectivement le Livre des procédures fiscales et le Code de procédure pénale.

... ET DE LA LOI CADA

Par ailleurs, les collectivités territoriales doivent répondre aux exigences de la loi « CADA » en matière d'accès aux documents administratifs. Également adoptée en 1978, cette loi a notamment pour objet de garantir la transparence de l'action publique. Le livre III du code des relations entre le public et l'administration reconnaît ainsi à toute personne le droit d'obtenir communication des documents détenus par une administration dans le cadre de sa mission de service public. Ce droit s'exerce à l'égard de toutes les personnes publiques (État, collectivités territoriales et établissements publics), mais aussi des organismes privés chargés d'une mission de service public. Si la loi permet par exemple à toute personne de demander à une collectivité la liste du personnel comprenant des éléments statutaires, tels que le grade et l'échelon de chaque agent public, elle prévoit toutefois quelques restrictions au droit d'accès, notamment pour préserver le respect de la vie privée des personnes ou le secret des affaires... Ainsi, la collectivité devra occulter la date de naissance et l'adresse personnelle des intéressés avant la communication du document sollicité, sauf à ce que celle-ci réponde à une obligation légale particulière dérogeant au régime général prévu par la loi « CADA » (par exemple, les dispositions relatives à la communication de la liste électorale ou des informations cadastrales).

A noter enfin que la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique est également venue apporter certaines nouveautés en matière de droit d'accès aux documents administratifs et de réutilisation des informations publiques. Elle vise notamment à renforcer ces droits en encourageant et en obligeant dans certains cas les collectivités publiques à diffuser sur Internet les documents librement communicables qu'elles détiennent. Toutefois, cette ouverture des informations publiques (« open data ») ne se fera pas en opposition au respect de la vie privée. En effet, sauf disposition légale contraire ou consentement préalable des personnes concernées, les informations contenant des données à caractère personnel ne pourront être publiées que si elles ont été au préalable anonymisées, sans risque de ré-identification des intéressés.

GS Mag : Quels sont les points clés de la réforme territoriale relatifs à ces problématiques ?

Alice de La Mure : La réforme territoriale implique une redistribution des compétences et donc des données d'usagers entre les différentes collectivités publiques impactées, ce qui peut s'avérer sensible en termes de sécurité et, plus largement, de protection des informations en cause. C'est pourquoi la CNIL a souhaité accompagner les collectivités dans la mise en œuvre de la réorganisation territoriale, afin que celles-ci tiennent compte des dispositions de la loi « Informatique et Libertés ». Pour ce faire, la CNIL a mis à disposition de ces organismes, dans la rubrique de son site Internet qui leur est dédiée des « check-lists » comprenant les étapes clés de la démarche à respecter, les différents points de vigilance et outils à utiliser... Il leur est ainsi notamment rappelé la nécessité d'identifier les données à transférer, la manière dont elles pourront garantir l'intégrité et la confidentialité des données transférées à l'occasion de leur transmission et dans le cadre de leur exploitation par la nouvelle collectivité compétente, ainsi que les modalités d'information des personnes concernées.

Le stade d'avancement de ces transferts/partages de compétences et de données s'avère actuellement très disparate d'une collectivité à l'autre. Beaucoup d'actions restent donc encore à réaliser en la matière.

AVEC LE RGPD, LE RÉGIME DÉCLARATIF LAISSE PLACE À LA GOUVERNANCE DES DONNÉES PERSONNELLES

GS Mag : Quelles évolutions le RGPD prévoit-il pour ces collectivités ?

Alice de La Mure : Les collectivités territoriales sont globalement logées à la même enseigne que les entreprises avec le nouveau règlement européen relatif à la protection des données personnelles, qui a été adopté en avril 2016 et qui entrera en application le 25 mai 2018. En plus de renforcer la transparence des traitements mis en œuvre et les droits des personnes concernées, le RGPD impose à l'ensemble des organismes de passer d'une logique de contrôle a priori, fondée sur la réalisation de formalités préalables, à une logique d'auto-

régulation, avec l'accompagnement et sous le contrôle de la CNIL dont le pouvoir répressif est largement « crédibilisé » (sanctions pécuniaires pouvant s'élever à 20 millions d'euros ou, pour une entreprise, à 4% du chiffre d'affaires mondial). Tenant compte du caractère particulièrement évolutif de l'univers numérique sur le plan des techniques comme des usages, il favorise une protection dynamique des données à caractère personnel et une responsabilisation de tous quant à ces problématiques. Les collectivités territoriales vont ainsi devoir prendre toutes les mesures techniques et organisationnelles permettant de garantir et de démontrer à tout instant un niveau de protection des données optimal.

Suivant cette nouvelle logique d'« accountability », le RGPD consacre deux nouveaux principes fondamentaux, à savoir la « Privacy by Design » (la protection de la vie privée dès la conception) et la « Privacy by default » (la protection de la vie privée par défaut). Les collectivités devront ainsi tenir compte le plus en amont possible, dès la phase de conception du produit, service, traitement, dès la phase de détermination des outils qui seront utilisés et des paramétrages par défaut, des droits et intérêts des individus. A titre d'exemple, il s'agira de favoriser par principe les menus déroulants ou les cases à cocher plutôt que les zones de commentaires libres sur les formulaires de collecte et dans les bases de données internes, pour cadrer, limiter dès le départ le nombre et la nature des données enregistrées ; de restreindre au maximum les droits d'accès informatiques aux données et les opérations susceptibles d'être réalisées ; de pseudonymiser les données toutes les fois où leur exploitation sous une forme identifiante n'apparaît pas nécessaire à la satisfaction du besoin ; ou encore d'appliquer un mécanisme automatique de purge des données à l'issue de la durée de conservation nécessaire à la réalisation de la finalité.
Conformément à cette logique de responsabilisation de l'ensemble des acteurs traitant des données personnelles, les situations juridiques des donneurs d'ordre et de leurs prestataires se trouvent rééquilibrées puisque les sous-traitants seront désormais également comptables du respect des grandes règles d'or de la protection des données. La CNIL pourra ainsi les sanctionner et leur responsabilité pourra également être engagée devant les juridictions par les personnes concernées.

Dans ce nouvel écosystème juridique, les collectivités comme leurs prestataires sont appelés à s'appuyer sur une large gamme d'instruments de conformité, à caractère obligatoire ou recommandé. Avec le RGPD, on assiste à un allègement considérable des obligations en matière de formalités préalables, puisque le régime déclaratif est totalement supprimé, pour rentrer dans l'ère de la gouvernance des données personnelles. Mais cette nouvelle ère va également être l'ère du formalisme, car une bonne gouvernance nécessite une documentation continue des réflexions et actions menées pour être en capacité de piloter et de démontrer la conformité. Les entreprises, comme les collectivités, seront ainsi amenées à formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des demandes de personnes tendant à l'exercice de leurs droits, à tenir un registre des traitements réalisés, à effectuer des analyses d'impact et à consulter la CNIL préalablement à la mise en œuvre des traitements présentant des risques élevés pour les personnes concernées, à adhérer à des codes de conduite, à certifier des traitements, et à notifier à la CNIL, voire aux personnes concernées, des violations de données... La désignation d'un délégué à la protection des données (Data Privacy Officer, DPO) constituera enfin une aide précieuse pour les collectivités bientôt confrontées à cette nouvelle donne.

TOUT ORGANISME PUBLIC DEVRA NOMMER UN DPO

GS Mag : Ont-elles l'obligation de désigner un DPO ? Si oui, quels sont vos conseils en la matière ?

Alice de La Mure : Tout organisme public devra, en effet, nommer un DPO. Dans la lignée du Correspondant Informatique & Libertés (CIL) actuel, dont la désignation est facultative, le DPO sera le « chef d'orchestre » de la conformité au sein de son organisme. Si le DPO reprend le statut et les attributions du CIL, on passe toutefois d'une fonction à un véritable métier, reconnu à part entière.

Le DPO aura pour principales missions :
- D'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- De diffuser une culture Informatique & Libertés au sein de la structure dans laquelle il exerce ;
- De contrôler le respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier ;
- De conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Dans l'exercice de ces missions, le DPO devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre. Pour garantir l'efficacité du pilotage de la conformité par le délégué, le RGPD prévoit qu'il devra être doté, sous peine de sanctions, d'un niveau d'expertise et de moyens renforcés. Ainsi, le DPO devra être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données. Il devra bénéficier d'un soutien important du responsable de traitement, en étant notamment associé en temps utile et de manière appropriée à l'ensemble des questions Informatique & Libertés. L'organisme devra, en outre, lui allouer les ressources et formations nécessaires pour mener à bien ses missions.

LA MUTUALISATION DE LA FONCTION DPO : UNE PISTE À PRIVILÉGIER POUR LES COLLECTIVITÉS

Dans ce contexte, la mutualisation de la fonction de DPO apparaît comme un enjeu essentiel pour les collectivités territoriales, notamment pour celles de petite taille qui ne disposent pas en interne des ressources nécessaires. A l'heure actuelle, 2/3 des régions ont désigné un CIL, 1 département sur 2, 2 métropoles sur 3, 1 communauté urbaine sur 2, 1 communauté d'agglomération sur 10 aussi, mais seulement

2% des communautés de communes et des communes.
Cette mutualisation de la fonction pourrait opportunément se faire au niveau de structures de mutualisation informatique, spécialisées dans le développement de l'e-administration sur leur territoire. De telles structures, qui ont vocation à se multiplier, couvrent déjà 50% des départements et permettent aux collectivités adhérentes de bénéficier d'un accompagnement dans l'informatisation de leurs activités, de rationaliser les dépenses tout en optimisant les conditions juridiques, organisationnelles et fonctionnelles du déploiement d'outils numériques de gestion de leurs missions de service public (ex. : développement de plateformes de téléservices). Elles constituent, en effet, des acteurs de choix pour cette mutualisation puisqu'elles regroupent maîtrise d'ouvrage et maîtrise d'œuvre et que c'est ainsi à leur niveau que sont identifiés les besoins, développés les progiciels utilisés, déterminés les mesures de sécurité, les paramétrages par défaut, voire hébergées les données.

L'ALPI (Agence landaise pour l'informatique) est ainsi déjà désignée pour plus de 70 communes, établissements publics et groupements de collectivités.

D'autres structures de coopération, et en particulier les communautés de communes, d'agglomération, les communautés urbaines et les métropoles, pourraient également travailler sur une offre de DPO mutualisé, qui donnerait aux collectivités qui y recourt l'assurance de bénéficier de l'expertise et de la disponibilité requise pour un exercice effectif des missions du délégué.

Enfin, il est à noter que quatre centres de gestion de la fonction publique territoriale proposent déjà des services de CIL mutualisés (CDG11, CDG54, CDG60 et le CDG59).

GS Mag : De manière générale, quelles sont vos recommandations pour assurer au mieux cette mise en conformité ?

Alice de La Mure : De nombreuses collectivités territoriales pâtissent encore d'une grande méconnaissance de leurs obligations en matière de protection des données. Un important travail reste donc à mener. Toutefois, la CNIL est à leurs côtés pour les aider à s'approprier le sujet et les accompagner dans leurs démarches de mise en conformité. Les collectivités peuvent ainsi trouver sur notre site, en particulier dans la rubrique « Collectivités territoriales », un certain nombre de guides et fiches pratiques, de normes et cadres de référence pour la mise en œuvre de leurs différents traitements (gestion de l'état civil, de la liste électorale, exploitation de systèmes d'information géographique, développement de téléservices, opérations de communication politique, etc.). Des outils y sont également à leur disposition, comme par exemple une méthodologie pour réaliser des analyses d'impact sur la vie privée et un catalogue de mesures à adopter pour les contrer ou limiter leurs effets. De plus, la CNIL travaille actuellement à l'élaboration d'un pack de conformité en matière d'open data, qui sera disponible vers la fin de l'année. Dans la rubrique « Règlement européen », les collectivités trouveront beaucoup d'informations sur la nouvelle règlementation, ainsi qu'un document intitulé « RGPD – Se préparer en 6 étapes ». Enfin, la CNIL propose de nombreux ateliers d'information généralistes et thématiques aux correspondants, pour leur offrir un accompagnement plus concret et pragmatique dans leurs démarches de mise en conformité.

CHAQUE COLLECTIVITÉ DOIT NOMMER UN CIL SANS ATTENDRE OU DÉTERMINER QUI POURRAIT OCCUPER CE POSTE

GS Mag : Quelles actions prioritaires les collectivités territoriales doivent-elles mettre en œuvre dès à présent ?

Alice de La Mure : Dans la mesure où les collectivités territoriales devront nommer un DPO pour se conformer au RGPD, il faut qu'elles anticipent dès à présent cette obligation en désignant sans attendre un CIL, qui deviendra DPO en 2018, ou au moins qu'elles commencent tout de suite à rechercher la personne qui aura vocation à occuper ce poste. Chaque collectivité doit, si ce n'est pas déjà fait, déterminer si elle dispose ou si elle pourrait ou non disposer des compétences en interne. Si ce n'est pas le cas, elle pourra alors contacter les structures environnantes susceptibles d'assumer ce rôle dans le cadre d'une mutualisation de la fonction (communautés de communes, communautés urbaines, agglomérations...). Sur le site de la CNIL, un fichier open data référence les collectivités territoriales ayant d'ores et déjà désigné un CIL, permettant de voir qui pourrait éventuellement mutualiser cette fonction.

Comme pour n'importe quel chantier, il faut qu'il y ait un chef chargé de coordonner les actions. Une fois ce pilote désigné, le reste se mettra en ordre de marche : sensibilisation des personnels, cartographie des traitements, évaluation des risques, priorisation des actions, organisation et outillage... Il est essentiel que chaque structure se donne les moyens pour parvenir à un niveau de conformité globalement satisfaisant, étant précisé que la date du 25 mai 2018 ne doit pas être vue comme un couperet ! La CNIL procédera prochainement à une communication auprès des différentes têtes de réseaux, des associations d'élus locaux en particulier, pour les sensibiliser au mieux à l'ensemble de leurs nouvelles obligations et leur rappeler son rôle d'accompagnement des collectivités dans la transition numérique, en même temps que de contrôle de la conformité de leurs traitements. ■■■

Pour en savoir plus :
Comprendre le règlement : https://www.cnil.fr/fr/comprendre-le-reglement-europeen
Se préparer en 6 étapes : https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes
Devenir délégué : https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

Par Bénédicte Pilliet, Directrice du CyberCercle and Co

LA CYBERSÉCURITÉ DOIT ÊTRE AU CŒUR DE LA CULTURE DES COLLECTIVITÉS TERRITORIALES

Le numérique est devenu un élément consubstantiel de notre société. Il touche tous les acteurs de la vie économique et sociale, privés comme publics, qui y voient un facteur de croissance et de prospérité, une facilitation des usages, que ce soit dans le cadre professionnel ou de la vie privée. Les collectivités territoriales n'échappent pas à cette transition numérique, bien au contraire. Toutefois, l'accession au numérique n'est pas sans danger et nécessite pour les collectivités territoriales d'insuffler une véritable culture de la cybersécurité à l'ensemble de leurs administrés.

A la jonction des sphères politique, économique et sociétale, les collectivités territoriales gèrent, par leur nature même, des systèmes d'information multiples et sont détentrices d'un volume important de données personnelles. Elles doivent également faire face à une accélération du process de modernisation de la vie publique, nécessitée par un cadre réglementaire qui s'accroît. Dématérialisation des échanges et des appels d'offre, signature électronique, open data, villes ou territoires intelligents, développement des concepts de e-administration et du e-citoyen, cadre de la Loi pour une République numérique... sont autant d'éléments qui poussent les collectivités territoriales à s'engager, parfois « à marche forcée », dans ces process de transition numérique. A cette évolution s'ajoute pour les territoires péri-urbains, et surtout ruraux, l'arrivée du THD, qui constitue un défi majeur pour leur développement à venir.

LE NUMÉRIQUE : UNE CHANCE POUR LES TERRITOIRES, MAIS NON DÉPOURVUE DE RISQUES...

Si le numérique représente, en effet, une chance de renforcer la proximité des institutions avec les citoyens, de faciliter les échanges avec les différents acteurs, publics et privés, qui participent à la vie des collectivités, au développement des activités et des territoires, il augmente en revanche, de fait, la surface de vulnérabilités des collectivités.

Vol de données des citoyens et des agents, sabotage des réseaux de gestion de l'eau, de l'éclairage public, détournement des services dématérialisés à destination de la population, vol ou modification des documents transitant

sur les réseaux, fraudes des appels d'offre dématérialisés, atteinte à l'image par défiguration de site, blocage des systèmes par un rançongiciel, détournement des systèmes de vidéosurveillance à des fins criminelles... sont autant de risques induits par un numérique où la sécurité a été trop longtemps mise de côté. Et l'est encore trop souvent.

Outre une actualité générale sur les cyberattaques, dont la dernière, massive, Wannacry, a bénéficié d'une médiatisation importante, les exemples ad hoc existent déjà, même si, comme pour beaucoup de structures attaquées, qu'elles soient publiques ou privées, la communication sur les cyberattaques subies reste souvent sporadique.

Défiguration de nombreux sites de collectivités sur les 21 000 touchés par la vague de cyberattaques « d'après Charlie » subie par la France en janvier 2015, attaque virale massive de type ransomware visant la ville de Vannes en février 2016, ransomware Locky touchant l'agence de l'eau Rhin-Meuse en septembre 2016... démontrent bien que les collectivités territoriales n'échappent pas aux cybercriminels.

Or, force est de constater que cette vulnérabilité numérique est peu prise en compte aujourd'hui par les élus ou les fonctionnaires territoriaux.
« La sécurité viendra dans un second temps » ; « Nous ne savons pas par quel bout le prendre » ; « Cela alourdit le process » ; « Cela coûte - trop - cher » ; « Nous ne sommes pas assez importants pour intéresser qui que ce soit »... sont autant de réflexions entendues lorsque l'on travaille avec des collectivités territoriales sur les questions de sécurité numérique. Réduite à sa seule dimension de ligne de coûts supplémentaires, la sécurité numérique est ainsi trop souvent, au pire, exclue du champ de la vie des collectivités, au mieux, restreinte à sa seule dimension technique.

LES COLLECTIVITÉS TERRITORIALES DOIVENT S'APPROPRIER LE CHAMP DE LA CYBERSÉCURITÉ...

Pour leur avenir, la sécurité de leurs concitoyens et de l'ensemble des acteurs présents sur leur territoire, il convient aujourd'hui que les collectivités territoriales s'approprient pleinement le champ de la sécurité numérique. L'un des leviers majeurs pour réussir ce défi serait que les dirigeants des collectivités, maires, présidents, adjoints au numérique, directeurs généraux des services... portent cette dimension et impulsent une dynamique interne. Contrairement aux idées reçues, la prise en compte de ce risque numérique n'est pas forcément fonction de la taille des collectivités : tout dépend de la prise de conscience du président de l'exécutif et de sa capacité à fédérer autour de cette dimension non seulement les responsables informatiques ou sécurité des systèmes d'information s'il y en a, mais également l'ensemble des services. Les services juridiques ont ainsi un rôle fondamental à jouer, tant les contraintes du cadre réglementaire pèsent aujourd'hui sur les dirigeants, avec en particulier l'application du Règlement Général sur la Protection des Données (RGPD) adopté en 2016 par l'Union européenne. Les services des Ressources Humaines a également un rôle prépondérant : outre la confidentialité des données qu'ils se doivent d'assurer, implémenter une culture partagée de la sécurité numérique à l'ensemble des agents devrait être un axe fort de la communication interne des collectivités. Le maillon faible est le plus souvent « entre le clavier et la chaise ». Aussi est-il indispensable de former aux « règles d'hygiène informatique » l'ensemble des acteurs qui ont à interagir sur les réseaux des collectivités afin de diminuer l'impact de ce facteur « humain » qui est aujourd'hui trop souvent le maillon faible du dispositif.

C'est dans cette optique qu'ont été créées en 2015 les journées « Cybersécurité et Territoires », à Fleurance dans le Gers. Associant réflexion stratégique, ateliers opérationnels tournés vers les préoccupations des acteurs présents sur les territoires, espace de rencontres et démonstrations, ces journées sont ainsi un cadre privilégié d'échanges et de formation au service des collectivités territoriales pour mieux appréhender les enjeux de la sécurité numérique et les aider à s'approprier les différents dispositifs qui sont à leur disposition. Elles permettent également à l'Agence Nationale de la Sécurité de l'Information (ANSSI) de valoriser le dispositif des référents territoriaux mis en place fin 2015.

Certes, la technologie va de plus en plus vite, les enjeux et les usages évoluent avec l'arrivée de nouvelles dimensions, telles que les objets connectés ou l'intelligence artificielle. Les cybercriminels s'adaptent avec un rythme tout aussi rapide, leurs ressources augmentent, leurs organisations se professionnalisent. Il ne sera pas possible de tout protéger. Mais engager sous l'impulsion de la tête de l'exécutif une réflexion stratégique globale associant les dimensions technique et organisationnelle, la gouvernance et la formation, au sein des collectivités territoriales est aujourd'hui indispensable pour permettre la réalisation de la e-démocratie et le développement des territoires par le numérique avec la dimension « confiance », qui seule peut leur assurer pérennité.

... MAIS AURONT BESOIN DE SOUTIEN

Bien évidemment, les collectivités territoriales ne peuvent faire cela seules, ne serait-ce que parce que 85% d'entre elles ont moins de 2 000 habitants, avec le niveau de ressources financières et humaines que cette dimension suppose. La mutualisation des ressources, une concertation entre les différents échelons des organisations territoriales, un dialogue renforcé avec les acteurs privés, mais aussi et surtout une véritable politique nationale publique de sécurité numérique pour aider les collectivités territoriales à assumer cette transformation représentent ainsi des enjeux majeurs pour la réussite de cet objectif ambitieux : faire des collectivités territoriales les fers de lance de la sécurité numérique des territoires, au service de la sécurité nationale. ■■■

Cybersécurité & Territoires

3ÈME ÉDITION - 6 et 7 JUILLET 2017 à FLEURANCE

Tables rondes

Espaces démos

Networking

Ateliers

AIRBUS

PYRÉNÉES GASCOGNE

CYBER CERCLE

FONDATION pour la RECHERCHE STRATÉGIQUE

Communauté de Communes Lomagne Gersoise

GRSD GASCOGNE

MINISTÈRE DE L'AGRICULTURE ET DE L'ALIMENTATION

PAYS PORTES DE GASCOGNE

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Ville de FLEURANCE

LE GROUPE LA POSTE

Gendarmerie nationale

Microsoft

CCI FRANCE

Interview de Fabrice Crasnier et Frédéric Stryjak, Pilotes de la RCC Occitanie
Par Marc Jacob et Emmanuelle Lamandé

RCC OCCITANIE : NOTRE OBJECTIF EST DE FAIRE DE LA CYBERDÉFENSE UNE PRIORITÉ NATIONALE

Créé en 2014, le relais de la Réserve Citoyenne Cyberdéfense (RCC) Occitanie compte déjà 15 membres volontaires. Il s'est fixé plusieurs missions pour sensibiliser, expliquer, débattre, proposer, organiser et susciter des évènements contribuant à faire de la cyberdéfense une priorité nationale.

Global Security Mag : Pouvez-vous nous présenter le relais RCC Occitanie ?

Fabrice Crasnier et Frédéric Stryjak : Créé en juin 2014, le relais RCC Occitanie se compose actuellement de 15 membres volontaires, dont quatre personnels d'active de la gendarmerie, un volontaire de la réserve opérationnelle scientifique et dix volontaires de la réserve citoyenne cyberdéfense.
Afin de répondre à l'ensemble des missions qui sont confiées au relais Occitanie de la Réserve Citoyenne Cyberdéfense, trois groupes, fonctionnant en totale symbiose, ont été créés au fur et à mesure des demandes. Chaque membre peut ainsi participer à un ou plusieurs groupes suivant son appétence et le temps qu'il peut y consacrer.

PLUS DE 50 ACTIONS DONT ÉTÉ MENÉES DEPUIS 2014

GS Mag : Quels sont vos objectifs ?

Fabrice Crasnier et Frédéric Stryjak : L'objectif est de sensibiliser, expliquer, débattre, proposer, organiser et susciter des évènements contribuant à faire de la cyberdéfense une priorité nationale, tout en concentrant l'action du réseau sur les aspects les plus régaliens et les volets les plus stratégiques.
A cette fin, **plus d'une cinquantaine d'actions ont été menées depuis 2014**. Durant le premier semestre de cette année, ce ne sont pas moins de 15 évènements auxquels la RCC a participé au profit d'écoles et de différentes Universités de Toulouse, ainsi qu'auprès d'associations. Elle a également pris part à des rencontres parlementaires sur des sujets, tels que le cyberharcèlement et les réseaux sociaux, le darknet et le cyberdjihadiste, l'usine 4.0 et les cybermenaces, ainsi que l'IoT, la robotique, le droit numérique, la maturité des entreprises et la cybercriminalité.

NOUS MENONS DES ACTIONS DE SENSIBILISATION ET D'ASSISTANCE AUX PME RÉGIONALES

GS Mag : Quels types d'actions menez-vous auprès des entreprises ?

Fabrice Crasnier et Frédéric Stryjak : La RCC Occitanie réalise des actions de sensibilisation et d'information auprès des sociétés. Notre action a toutefois évolué vers la maturité

Colloques

Groupement entreprise

Collèges, lycées & universités

Institutionnels

des entreprises demanderesses à l'aide des outils de l'ANSSI et de notre tableau de bord de sensibilisation. L'action collective Aerospace Valley, à laquelle participaient tous les services de l'État (DGSI, DRSD, Gendarmerie, DIRRECTE et RCC Occitanie), fut présentée en 2015 à une centaine de chefs d'entreprises et de managers de la sécurité. Cette manifestation a sonné le point de départ de nos analyses de maturité. En effet, après chaque conférence, une seule interrogation jaillissait : « Concrètement, nous faisons quoi et qu'avez-vous à nous proposer ? ». Le fait d'avoir réuni en son sein toutes les compétences nécessaires (informatique, managériale, juridique et sociale) pour remplir ses missions, la RCC Occitanie a pu répondre aux appels de détresse des entreprises de la région. Chemin faisant, nos actions altruistes ont permis de mettre en confiance tous les services de l'État de la région qui nous ont confié une part de leur action sur ce volet. Toutefois, nous avons bien conscience de ne pas être là pour remplacer quiconque et il a été important de se fixer des limites, même si l'enthousiasme et les compétences de nos membres vont parfois bien au-delà. Toujours en quête d'amélioration, et poursuivant notre sacerdoce en prenant un soin tout particulier au conflit d'intérêt qui pourrait être mal interprété, nous avons porté notre modèle à l'extérieur de la région par des sollicitations. Enfin, le 1er mars 2017, nous avons eu l'honneur de recevoir M. Guillaume Poupard, Directeur général de l'ANSSI, M. Pierre Gacic, Chef du bureau de coordination territoriale de l'ANSSI, ainsi que M. Yves Jussot, Référent ANSSI en territoire Occitanie.
A ce jour, plus d'une dizaine d'entreprises ont été visitées tant sur la région toulousaine que sur la région aveyronnaise. La satisfaction des membres de la RCC a été à leur comble devant l'enthousiasme des remerciements des dirigeants de ces sociétés. La RCC Occitanie vient de clore la réalisation des analyses de maturité à la sécurité informatique, réalisées au profit des sociétés adhérentes au pôle de compétitivité Aerospace Valley dans le cadre du volet 2 de l'action collective cybersécurité, piloté par la DIRECCTE Toulouse et Aerospace Valley.

La RCC Occitanie, ainsi que les services régionaux de la DRSD, la DGSI ou encore l'ANSSI se sont partagés les sociétés qui se sont portées volontaires lors de la sensibilisation constituant le volet 1 de de cette action. **Pas moins de 12 analyses ont été réalisées par la RCC Occitanie entre 2016 et 2017.** Il s'agit principalement de PME, mais aussi de TPE, pour la plupart en lien avec le monde aéronautique. Les équipes de réservistes citoyens cyber de la région Occitanie se sont déplacées principalement en Haute-Garonne, mais également dans le Gers ou encore l'Aveyron. Rappelons que l'analyse dite de maturité à la sécurité informatique est réalisée à partir d'un questionnaire reprenant les recommandations de l'ANSSI et permet, à l'issue des deux heures de débats nécessaires, d'apporter aux dirigeants un éclairage sur les points forts comme les points faibles de leurs systèmes d'information. La qualité du travail, tout comme l'engagement des réservistes citoyens en charge des analyses ont fait l'objet de nombreux éloges de la part des dirigeants.

NOUS AVONS ENRICHI NOS OUTILS DE COMMUNICATION AVEC DU CHIFFREMENT

GS Mag : Quels outils de communication utilisez-vous ?

Fabrice Crasnier et Frédéric Stryjak : L'objectif est d'enrichir nos outils de communication avec des éléments locaux. Il s'agit également de créer de nouveaux outils applicables à la cyberaérodéfense, mais aussi de faire la différence par l'innovation de produits de sensibilisation faisant appel à des compétences particulières. Nous avons d'abord mis en place les **outils de communication sécurisés entre les membres de la RCC** (messagerie sécurisée IMAP HTTPS, réseau VPN pour accéder aux services Intranet RCC Occitanie offrant un accès au serveur Web RCC Occitanie et au Cloud RCC Occitanie) sur les ordinateurs fixes, portables et les smartphones. Ensuite, nous nous sommes attachés à sécuriser la communication entre le relais RCC Occitanie et les entreprises, par l'**usage de conteneurs chiffrés**, attachés en pièce jointe de nos messages à destination des entreprises et l'**usage d'un certificat pour la signature numérique** des messages contenant une pièce jointe. L'objectif est, en effet, de se sécuriser et de former nos interlocuteurs à la sécurité de base. De plus, pour répondre aux sollicitations de différents colloques, nous avons également **développé des « pots de miel »** afin d'attirer l'attention sur notre capacité et notre technicité dans les domaines innovants.

Enfin, pour répondre à la demande de la Gendarmerie et du CROEGN, cinq membres de la RCC Occitanie participent aux groupes de travail suivants :
- Enjeux des systèmes connectés pour les forces de sécurité : le cas particulier de la domotique ;
- Conception d'un vade-mecum sur les liens entre la Gendarmerie et les collectivités territoriales en matière de cybersécurité. ■■■

Par Jean-Paul Mazoyer, Directeur du Crédit Agricole Pyrénées Gascogne

NOTRE RÔLE DE BANQUE RÉGIONALE MUTUALISTE EST D'AIDER LES ACTEURS DU TERRITOIRE À RÉUSSIR LEUR TRANSFORMATION NUMÉRIQUE

Le système bancaire français compte de nombreuses banques mutualistes (Crédit Agricole, banques Populaires, Caisses d'Epargne, Crédit Mutuel). La finalité de ces établissements bancaires, qui enregistrent fréquemment des parts de marché très élevées dans les territoires où ils opèrent, est d'aider les acteurs économiques de nos régions à s'adapter, à préparer leur avenir. Bien évidemment, la recherche d'un profit à leurs actions ne leur est pas étrangère. Mais le résultat net de ces entreprises bancaires, souvent mis en réserve dans sa quasi-intégralité, est un moyen de poursuivre le développement et non une finalité pour rémunérer le capital : c'est là toute la différence de ce mouvement mutualiste.

L'utilité concrète à nos territoires, credo fort des banques régionales mutualistes, se traduit aujourd'hui autour des transitions économiques, énergétiques et évidemment numériques : comment ces banques peuvent-elles aider les acteurs économiques (entreprises, professionnels, agriculteurs, collectivités locales...) à se saisir de ces sujets et à réussir leur mutation ? Comment faciliter ces transitions ?

La réalité de ces banques régionales mutualistes (nous parlons ici d'entreprises qui emploient plusieurs milliers de salariés chacune) est qu'elles sont elles-mêmes confrontées à la nécessaire adaptation de leur fonctionnement et de leur système de relations avec leurs clients. Sous le quadruple effet i) du changement de comportements des consommateurs, ii) de la diffusion généralisée des nouvelles technologies, iii) de la démographie de leurs salariés, et iv) des contraintes règlementaires croissantes, ces établissements financiers s'adaptent et se transforment. Sans être nécessairement exemplaires, elles n'en ont pas moins une certaine expérience des ruptures en jeu. Et compte tenu de l'importance des systèmes d'information dans les entreprises bancaires, les indispensables adaptations liées à la révolution numérique leur sont familières.

Ces banques régionales mutualistes sont fréquemment les premiers pourvoyeurs de crédit à l'économie de nos territoires. Et de façon très pragmatique, une entreprise, un professionnel, un artisan qui s'adapte aux nouveaux enjeux constitue un risque moindre pour le prêteur. Ces banques ont donc tout intérêt à aider leurs clients à s'adapter, ne serait-ce que pour leurs propres ratios de risque. La santé financière de ces banques totalement ancrées dans les territoires est, par nature, fortement corrélée au dynamisme économique de la région et à la santé financière de ses acteurs.

CES BANQUES FAVORISENT LA MISE EN RELATION ENTRE LES CLIENTS ET LE SOUTIEN DES INITIATIVES LOCALES

Alors que peuvent faire ces banques pour faciliter ces transitions ? Beaucoup de pédagogie, beaucoup de mise en relation entre les clients, beaucoup d'explications et beaucoup de soutien aux initiatives locales...

A titre d'illustration, on citera cette banque qui organise, sur son territoire, des cafés de la transition numérique dans l'agriculture, où des agriculteurs en avance viennent expliquer à d'autres agriculteurs intéressés à comprendre tout l'apport des technologies dans ce domaine. Et tout cela avec l'aide de fournisseurs informatiques.

On pourra citer ce sénateur d'un département rural qui organise, avec l'aide d'une banque régionale mutualiste, un colloque annuel réunissant toutes les autorités françaises en matière de cybersécurité. Dénommé « Cybersécurité et Territoires », ce colloque a pour vocation de contribuer à la prévention des risques informatiques.

Ou encore, ce dispositif national toujours lié à la cybersécurité, relayé sur les territoires par les tiers de confiance que sont les banques, et qui vise à expliquer les risques et à assister, en cas d'attaque, les acteurs économiques de nos régions.

Les acteurs économiques de nos régions, si l'on exclut les établissements de nos grandes entreprises nationales, sont souvent de petites ou moyennes entreprises, des entreprises de taille intermédiaire ou des professionnels qui se retrouvent fréquemment isolés face à ces enjeux de transformations numériques et, de façon encore plus prégnante, face aux risques de cybersécurité.

C'est la responsabilité de ces acteurs économiques locaux que sont les banques régionales mutualistes, qui disposent de compétences et de moyens plus importants, de contribuer, par leur engagement, à la transition de nos territoires. ■■■

PUBLI INFO

VOS EFFORTS DE SÉCURISATION SONT-ILS EFFICACES ?

Alain SCHNEIDER,
Président et Consultant, COGICEO

Les responsables de systèmes d'information ont aujourd'hui pris conscience de l'importance de sécuriser leurs périmètres. La plupart a également engagé des chantiers en ce sens. Cependant, beaucoup d'entre eux dirigent leurs efforts dans de mauvaises directions, faute de retour objectif sur le niveau de sécurité atteint.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

Les collectivités territoriales, ainsi que les ETI se trouvent à la croisée des chemins. Elles manipulent assez d'informations et/ou d'argent pour intéresser les cyber-délinquants, mais n'ont pas toujours des moyens conséquents pour mettre en œuvre leur sécurité. De plus, pour beaucoup d'entre elles, la sécurité est une préoccupation relativement nouvelle, or ce n'est pas un sujet facile à prendre en main.
La prise de conscience d'un besoin de sécurité est un premier pas déjà franchi chez la plupart des collectivités territoriales et des ETI. De même, nombreux sont ceux qui ont d'ores et déjà effectué leurs premières actions concrètes vers la sécurisation du SI, aussi timides soient-elles. En revanche, rares sont ceux qui ont réussi à nouer des relations de collaboration solides avec un prestataire externe capable de les aider de façon efficace. Les ETI et les collectivités territoriales pourraient pourtant grandement profiter d'une aide extérieure expérimentée capable de leur apporter une vision objective des progrès qu'elles réalisent. En effet, une mesure objective de l'efficacité des mesures prises fait souvent défaut aux décideurs qui risquent alors de se lancer dans des chantiers coûteux, mais finalement peu pertinents dans leur contexte (les mesures de sécurisation les plus pertinentes ne seront pas les mêmes dans une entreprise du CAC 40 que dans une collectivité territoriale).
Afin d'éviter ces chantiers inutiles, il suffirait que le plan d'action se nourrisse de recommandations issues d'audits externes réalisés par un spécialiste, mais trouver un prestataire spécialisé en sécurité et capable d'intervenir hors du contexte des multinationales reste une gageure. En effet, identifier des partenaires à la fois agiles, compétents et à l'écoute, avec lesquels des structures de la taille des ETI ou des collectivités territoriales peuvent nouer des relations de travail bénéfiques et durables est un véritable défi tant l'espace médiatique est encombré par quelques colosses du conseil ayant récemment décidé de s'engager sur le secteur de la sécurité des SI.

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

Chez COGICEO, nous essayons d'aller à la rencontre de toutes les personnes ayant à cœur d'améliorer la sécurité des systèmes d'information dont elles ont la responsabilité. Sans discrimination de taille, de budget ou de niveau de maturité. Ainsi, nous avons le plaisir de compter parmi nos clients fidèles aussi bien des TPE que des entreprises du CAC 40 très attachées à notre qualification PASSI. Les audits de sécurité que nous réalisons s'étalent donc de l'intrusion « red team » multi-modale sur plusieurs mois aux rapides audits semi-automatiques de domaines Microsoft. Les premiers sont des outils essentiels pour nos clients les plus matures qui souhaitent mettre à l'épreuve l'ensemble des systèmes qu'ils ont mis en place ; les seconds constituent une base saine et peu coûteuse sur laquelle commencer à bâtir la sécurité d'un SI bureautique.

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

Pour accompagner la croissance des périmètres de sécurisation de nos clients, nous avons étendu la couverture de nos audits semi-automatiques de domaine Microsoft. Il y a 3 ans, nous n'analysions que le serveur central, afin d'établir nos recommandations de sécurisation de ce dernier et du domaine qu'il régit. Aujourd'hui, de plus en plus de nos clients commencent à maîtriser la sécurité de ce cœur de réseau. Nous avons donc fait évoluer nos outils et proposons à présent d'auditer chacun des serveurs constituant le domaine en plus du contrôleur central, qu'ils soient une poignée ou plusieurs dizaines de milliers.
De même, nous travaillons à rendre nos rapports d'audits aussi pédagogiques que possible. Nous pensons qu'un audit n'a d'intérêt que s'il sert de guide vers une sécurité plus élevée. Or, pour qu'un guide soit efficace, il doit être compréhensible et adapté aux moyens de celui qui doit le suivre. ■■■

INFORMATIONS PRATIQUES

→Solution phare
ADAnalyzer, la solution semi-automatique d'audit de domaines Microsoft permet de rapidement visualiser le niveau de sécurité actuel, son évolution au cours du temps et les chantiers de sécurité à mener en priorité.

→Contact
Alain SCHNEIDER
→Téléphone
+33 (0)1 85 08 10 70
→Courriel
contact@cogiceo.com
→Web
www.cogiceo.com

COGICEO

PUBLI INFO

LA DÉTECTION
DES VULNÉRABILITÉS EST UN MUST

Maxime ALAY-EDDINE,
Président fondateur de Cyberwatch

Aujourd'hui, toute organisation reste sous la menace de cyberattaques, comme l'a démontré tout récemment Wannacry. L'ANSSI recommande d'ailleurs de mettre régulièrement à jour ses systèmes et logiciels. Dans cette optique, Cyberwatch a développé un logiciel de détection et de supervision des vulnérabilités, qui permet d'améliorer le niveau de sécurité des systèmes d'exploitation par l'administration continue des vulnérabilités (24/24 et 7/7).

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

Les collectivités et les ETI sont confrontées aux mêmes enjeux en matière de cybersécurité que les grands groupes (destruction et vol de données, espionnage industriel, escroqueries économiques, sabotage de sites Web…), bien que disposant de moins de moyens techniques et financiers.
Ces organisations prennent de plus en plus la mesure du risque et savent maintenant qu'une attaque informatique peut être très préjudiciable au niveau de l'image, de la disponibilité des systèmes, du vol de données, et que les conséquences financières sont de plus en plus lourdes, en particulier dans le cadre du Règlement Général sur la Protection des Données (RGPD).
Je vous rappelle que dans tous les systèmes d'exploitation et logiciels, il existe des défauts de fabrication, appelés vulnérabilités, qui sont autant d'opportunités pour les pirates. Dès que les éditeurs découvrent ces défauts, ils procèdent très vite à leur correction. Il est donc essentiel pour toute organisation de connaître l'état de son parc vis-à-vis de ces vulnérabilités et de procéder à leur correction.
Wannacry est un douloureux rappel qui a cependant pour bénéfice d'informer, de sensibiliser et de mobiliser les organisations et les incite à mieux se protéger. Beaucoup de collectivités et entreprises parmi nos prospects ont pris conscience que ce virus n'avait d'impact que si des vulnérabilités connues n'avaient pas été traitées.

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

L'ANSSI recommande aux organisations de mettre à jour leurs systèmes et logiciels, c'est pour elle une priorité. Partant de cette préconisation et constatant que beaucoup d'organisations, publiques comme privées, sont très souvent en retard sur ce point, Cyberwatch a développé un logiciel, 100% français, de détection et supervision des vulnérabilités qui permet d'améliorer le niveau de sécurité des systèmes d'exploitation par l'administration continue des vulnérabilités (24/24 et 7/7).
Cette application multiplateforme (Windows, Linux) possède son propre moteur de détection et s'installe rapidement, avec ou sans agent.
Cyberwatch s'adapte à l'environnement existant (infogérance, WSUS, politique de sécurité existante…) et fournit les outils de supervision participant au maintien de condition de sécurité.
Cyberwatch génère des tableaux de bord qui fournissent une information pertinente prenant en compte le niveau de sévérité des vulnérabilités, la criticité des serveurs et l'existence d'exploit.
Cyberwatch embarque, sur option, un outil de planification et de déploiement des correctifs de sécurité. Dans le cas de Wannacry, nos clients ont su dès le 15 mars que des vulnérabilités graves devaient être traitées par des mises à jour système. Certains clients utilisent également notre module intégré de Patch Management et étaient alors à l'abri de Wannacry dès le 15 mars au soir.

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

L'axe de développement que nous avons choisi nous semble pérenne et nous souhaitons donc renforcer notre efficacité dans la prévention des risques au travers de la gestion et correction des vulnérabilités.
Nous devrions, à court terme, développer de nouvelles fonctionnalités pour aider nos clients à prioriser leurs actions en fonction de la gravité des vulnérabilités existantes.
Rapidement, nous souhaitons élargir le périmètre de notre logiciel aux matériels réseaux, aux postes de travail et plus tard aux objets connectés. ■■■

INFORMATIONS PRATIQUES

→Solution phare
Logiciel de détection et supervision des vulnérabilités

→Contact
Maxime ALAY-EDDINE
→Téléphone
+33 (0)6 25 23 64 81
→Courriel
maxime@cyberwatch.fr
→Web
www.cyberwatch.fr

Cyberwatch
cybersecurity as a service

PUBLI INFO

MAITRISEZ VOTRE CYBERSÉCURITÉ EN TOUTE AGILITÉ

Jean LARROUMETS,
PDG d'EGERIE Software

Au regard des incidents et cyber-attaques survenus récemment et des règlementations toujours plus nombreuses et contraignantes dans le domaine, comme la LPM, le RGS, ou le GDPR pour ne citer qu'elles, les collectivités territoriales comme les ETI sont maintenant dans l'obligation de prendre la main sur leur cybersécurité et d'en assurer la maîtrise globale si elles ne veulent pas mettre en péril leur image, leurs intérêts ou leur activité.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

Les collectivités territoriales comme les ETI sont maintenant tout autant exposées aux cyber-menaces que les grands comptes, l'exemple de Wannacry l'a récemment démontré. La maîtrise complète de leur cybersécurité devient une priorité. Toute vulnérabilité technique ou non technique, humaine, procédurale ou physique non traitée est source de risques et de problèmes directs pour ces structures.
Bon nombre de collectivités ou ETI n'ont malheureusement pas encore pris la mesure de cet enjeu et n'ont pas une approche globale de leur cybersécurité laissant ainsi des brèches qui les exposent fortement, tant à des cyberattaques qu'à des sanctions règlementaires.
Les plus matures ont commencé à poser les fondations et les premières pierres de ce processus vertueux de sécurisation en conformité avec les standards et règlementations, mais elles peinent souvent à le maintenir dans la durée et à le généraliser.

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

Les solutions EGERIE leur permettent d'initier facilement cette démarche et, pour les plus matures, de mettre en place une vraie politique de gouvernance des risques cyber en intégrant les principaux référentiels : Secteur public (Loi de Programmation Militaire pour les OIV, PSSI-E, RGS), Réglementation Défense (IGI, OTAN…), Secteur Energie (CEI 62645 et REGULATORY GUIDE 5.71), Secteur Santé (Hôpital Numérique), Hébergement de données.
Grâce à sa technologie de pointe, son moteur d'analyse et ses bibliothèques métiers et normatives, la suite EGERIE élabore la cartographie des cyber-risques et la gouvernance Privacy/GDPR de l'entreprise. Elle rationalise, de plus, la stratégie cybersécurité et privacy à définir, à mettre en œuvre et à maintenir.
Sa plate-forme centralisée et collaborative permet d'intégrer facilement chaque nouveau système ou projet dans la démarche de Cybersécurité de l'entreprise et d'en assurer le suivi global en impliquant l'ensemble des collaborateurs clés. Notre suite logicielle se décline en deux produits complémentaires :

- EGERIE RiskManager, notre produit phare, permet d'identifier très rapidement les risques d'incident cyber sur la structure grâce à son moteur d'analyse qui construit dynamiquement à la fois la cartographie des risques, mais aussi les moyens de les traiter, selon l'état de l'art méthodologique. Ses indicateurs et tableaux de bord dynamiques donnent aux acteurs clés de l'entreprise une vision claire, précise et toujours actualisée de leur niveau de cybersécurité (Risques et Impacts actuels et potentiels, État des lieux des Mesures de sécurité sur la structure, Vulnérabilités résiduelles et Conformité réglementaire).
- EGERIE PrivacyManager permet la conformité avec le nouveau règlement européen sur la Protection des données (RGPD / GDPR) 2016/679, tout en assurant la mise en place d'une gouvernance Data Privacy collaborative, ultra-performante incluant l'évaluation du risque et l'analyse d'impact (modélisation des données et processus avec référentiel GDPR pré-intégré, évaluation des risques et analyse d'impact, gestion des registres et production des rapports de conformité).

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

Nos solutions sont évolutives et enrichies de façon régulière grâce à la vision portée par EGERIE et les contributions dynamiques du club utilisateur.
Nous nous appuyons sur un réseau de partenaires certifiés pour accompagner nos clients dans leur mise en conformité règlementaire, et les guidons avec nos solutions EGERIE RiskManager et PrivacyManager vers une gouvernance optimale et pérenne. ■■■

INFORMATIONS PRATIQUES

→Solution phare
RiskManager pour le RSSI
PrivacyManager pour le DPO

→Contact
Marion THOMAS
→Téléphone
+33 (0)1 43 87 70 28
→Courriel
contact@egerie-software.com
→Web
www.egerie-software.com

EGERIE

PUBLI INFO

ACCUEILLEZ L'INNOVATION AVEC LES SOLUTIONS QUI VOUS PERMETTENT DE LE FAIRE EN TOUTE SÉCURITÉ

Florian MALECKI,
International Product Marketing Director, SonicWall

En allant au-delà de la détection des failles de sécurité, SonicWall fournit une solution de prévention des menaces proactive en temps réel qui permet de protéger les entreprises contre les cyber attaques, notamment les ransomwares, les attaques IoT DDoS et les malwares cachés dans le trafic encrypté.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

D'après le dernier rapport des menaces de SonicWall, le nombre d'attaques de type ransomware a été multiplié par 167 par rapport à l'année précédente, et la dernière en date WannaCry a malheureusement bien illustré ce phénomène. Le trafic encrypté a, quant à lui, augmenté de 38 % d'une année sur l'autre, favorisant ainsi le développement des cyber menaces cachées dans ces flux chiffrés. Aussi, les objets connectés ont créé un nouveau vecteur d'attaques, ouvrant la porte à celles par DDoS à grand échelle. Rajoutez à tout cela les différents règlements comme le RGPD, qui entrera en vigueur dès le mois de mai 2018, les sociétés et autres organismes publics ont fort à faire en matière de sécurité informatique !
Les auteurs des attaques exploitent, en outre, toutes les opportunités que leur offre l'automatisation et font évoluer leurs menaces dans un seul objectif : lancer des attaques de la plus grande ampleur possible en évitant toute détection. Étant donné l'impact terrible de toute fuite de données ou d'attaque par ransomware pour les entreprises, la prévention des menaces proactive en temps réel est un impératif pour les organisations.

GS Mag : Comment se protéger et bloquer ces attaques ?

Les pare-feux de nouvelle génération intègrent des fonctionnalités de sécurité automatisées et dynamiques au sein d'une même et unique plateforme, afin de bloquer les menaces les plus complexes :

- La protection antivirus et anti-logiciels espions certifiée ICSA offre un anti-malware au niveau réseau, pour une sécurité approfondie contre les menaces évoluées modernes.
- La technologie IPS d'avant-garde protège contre les vers, chevaux de Troie, vulnérabilités logicielles et autres intrusions en scannant l'ensemble du trafic à la recherche de comportements malveillants ou anormaux, ce qui augmente la fiabilité et les performances du réseau.
- Application Intelligence and Control réunit un ensemble de règles granulaires, spécifiques aux applications, qui permettent de classifier ces dernières et aident les administrateurs à contrôler et à gérer toutes les applications, qu'elles soient à caractère professionnel ou privé.
- À des fins de sécurité et de productivité, le filtrage de contenu offre les contrôles permettant d'appliquer des règles d'utilisation d'Internet et de bloquer l'accès aux contenus Web nuisibles et non productifs.
- Sandboxing : en plus de passer le code au crible pour y trouver des signatures ou des indices d'intentions malveillantes connus, une sandbox permet d'activer un code normalement et de surveiller son comportement obtenu afin d'y déceler toute activité malveillante et ainsi bloquer l'attaque. On utilise pour cela un environnement spécial, dans laquelle votre système ne risque rien.

GS Mag : Comment votre gamme de solutions peut-elle aider les collectivités territoriales et les ETI à protéger leur réseau ?

Les pare-feux de nouvelle génération SonicWall bloquent efficacement les ransomwares et autres types d'attaques avec une approche multicouche - GAV, IPS, Filtrage de contenu - qui s'ajoute à la solution de sanboxing basée sur plusieurs moteurs : SonicWall Capture Advanced Threat Protection Service. Capture scanne une grande variété de types de fichiers pour détecter les menaces avancées, grâce à une analyse en parallèle des trois moteurs, les bloque avant d'obtenir un verdict de sécurité et déploie rapidement les signatures de correction. Cela garantit une sécurité beaucoup plus efficace, des temps de réponses plus rapides et un coût total de possession réduit.
SonicWall Email Security avec Capture ATP offre une inspection du trafic basé sur SMTP encore plus approfondie et plus transparente pour l'utilisateur. Pour bloquer les ransomwares provenant des appareils mobiles, les flux venant de la solution SonicWall Secure Mobile Access sont analysés par le pare-feu SonicWall, afin de procéder à une analyse plus poussée.
SonicWall aide les entreprises à prévenir les attaques causées par des malwares et autres menaces provenant du trafic chiffré, en offrant des performances d'inspection du trafic SSL, TLS et SSH en temps réel les plus élevées de leur catégorie. ■■■

INFORMATIONS PRATIQUES

→Solution phare
SonicWall Capture Advanced Threat Protection

→Contact
David HADDAD
→Courriel
france@sonicwall.com
→Web
www.sonicwall.com

SONICWALL®

PUBLI INFO

SOPHOS CENTRAL : UNE PROTECTION COMPLÈTE ET SYNCHRONISÉE DES SYSTÈMES ET DES RÉSEAUX

Michel LANASPEZE,
Directeur Marketing pour l'Europe de l'Ouest, SOPHOS

Les ETI et les collectivités territoriales ne disposent souvent que d'équipes restreintes pour assurer et maintenir un très haut niveau de sécurité. C'est pourquoi Sophos leur propose une protection complète, simple à mettre en œuvre et synchronisée de leurs systèmes et réseaux via sa solution Sophos Central.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

De par leurs tailles et leurs activités, les ETI et les collectivités territoriales sont tout autant exposées aux cyberattaques modernes que les grands groupes. Elles ont donc vocation à se protéger avec un éventail de techniques de protection tout aussi large et complet. Cependant, elles ne bénéficient ni des mêmes moyens, ni d'experts aussi nombreux pour les mettre en œuvre. Il est donc essentiel qu'elles disposent de solutions qui leur apportent à la fois une protection de pointe, complète et simple à mettre en œuvre.

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

Grâce à plus de 30 années d'expertise dans le domaine de la sécurité, Sophos a développé des protections particulièrement complètes aussi bien pour les systèmes, la mobilité et les données, que les réseaux. Ces protections sont à la pointe de la lutte contre les attaques modernes, telles que les ransomwares ou l'exploitation des vulnérabilités, et intègrent les technologies NextGen les plus avancées. Par ailleurs, Sophos investit depuis très longtemps dans la simplicité et l'intégration de ses solutions pour apporter une réponse performante, complète et modulaire, parfaitement adaptée aux exigences et aux contraintes des ETI et des collectivités territoriales. Elles permettent à des équipes restreintes de pouvoir assurer et maintenir un très haut niveau de sécurité, grâce à des fonctions avancées auxquelles elles n'auraient pas accès autrement.

Par exemple, les technologies de protection NextGen apportées par Intercept X, qui assurent une protection avancée contre les ransomwares et l'exploitation des vulnérabilités, et qui ont montré toute leur efficacité contre les attaques WannaCry, peuvent aussi bien se déployer isolément, en complément d'une solution de protection Endpoint tierce existante, que dans le cadre de la console Sophos Central, qui assure cohérence et communication entre la gestion de la sécurité des postes, des serveurs, des mobiles, des données, de la messagerie, du Web, du WiFi et du réseau.

Dans ce cadre, la synchronisation dynamique et en temps réel de la sécurité entre le réseau et les systèmes permet de détecter des attaques qui passeraient inaperçues autrement. Le pare-feu peut ainsi obtenir des informations détaillées sur les sources de trafic qu'il n'arriverait pas à identifier sinon. Il peut également surveiller l'état de santé des postes, pour détecter si une protection a été désactivée par un malware ou par négligence. Il peut également identifier avec précision et immédiatement tout processus qui se mettrait à générer un trafic malveillant, afin de le neutraliser immédiatement et de rechercher sa présence éventuelle sur d'autres postes. Ceci permet de mettre en place des actions de remédiation automatiques, qui nécessiteraient sinon de longues heures d'examens et de recoupements manuels.

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

Cette synchronisation ne fait que commencer à montrer tout son potentiel. Le dialogue entre la protection des postes et le chiffrement permet par exemple de supprimer automatiquement les clés de chiffrement sur un poste compromis, le temps de remédier au problème, pour éviter la fuite d'informations sensibles. Nous ajoutons ainsi de nouvelles capacités très régulièrement.

Nous avons récemment ajouté à Sophos Central notre solution de gestion et de protection des mobiles. Sophos Central permet ainsi de gérer la sécurité des postes, des mobiles et des données d'un même utilisateur d'une manière simple, cohérente et intégrée.

De nouvelles technologies, issues de nos acquisitions récentes de sociétés pionnières dans les domaines de la corrélation d'information (Forensics) et de l'apprentissage machine (Deep Learning) viendront bientôt se rajouter à Sophos Central, pour assurer une protection toujours à la pointe de la lutte contre les menaces les plus avancées. ■■■

INFORMATIONS PRATIQUES

→Solution phare
Sophos Central

→Contact
Bruno LECLERC
→Téléphone
+33 (0)1 34 34 80 37
→Courriel
bruno.leclerc@sophos.fr
→Web
www.sophos.fr

SOPHOS
Security made simple.

PUBLI INFO

eGambit, LE CYBER ARSENAL DÉFENSIF FRANÇAIS

Laurent OUDOT,
co-CEO & CTO de TEHTRIS

Les techniques et les actions offensives se multiplient pendant que les défenses classiques vacillent. Se mettre en conformité face aux vraies menaces devient très compliqué et réellement coûteux. Peut-on se réapproprier une défense informatique de manière modulaire, souple et efficiente, qui prend en compte le passé et le futur, avec une capacité de surveillance et de protection à la hauteur ? C'est dans cet esprit que notre société, TEHTRIS, conçoit et déploie eGambit dans le monde entier au service d'entités de toutes tailles. Un succès scientifique.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

Pendant des années, les menaces techniques essentielles semblaient orientées sur les grandes infrastructures, états et multinationales, au-delà des attaques hasardeuses de virus et *worms*. Nous vivions une fausse période de paix, où les éléments classiques de défense comme par exemple l'antivirus, les mises à jour, les firewalls et le proxy semblaient suffire, sans parler d'une réactivité sommaire. Seul problème : la paix n'est plus, et les technologies désuètes ne suffisent pas à se protéger et à surveiller son environnement. L'accélération technologique des moyens offensifs n'est pas toujours prise en compte de manière globale, que ce soit pour les collectivités territoriales ou les ETI, et même au-delà. Par ailleurs, le marketing à outrance n'a pas aidé, et nombreux sont ceux qui regrettent que certains produits et services ne furent pas au rendez-vous lors des grandes attaques récentes. Nous avons actuellement des besoins d'efficacité à des coûts raisonnables, offrant l'accès à des éléments scientifiques orientés terrain, et réalité.

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

Grâce à notre technologie eGambit, nous avons considérablement simplifié l'équation et réduit les coûts associés, offrant une cybersécurité efficiente. Au lieu de sombrer dans les rachats de technologies, les levées de fond et le monde du buzz, les experts français de TEHTRIS passèrent plusieurs années à coder de nombreuses briques interconnectées, offrant une vision à 360° à nos clients, dans un mode SaaS apprécié qui simplifie les déploiements et la souplesse de l'usage. Quelles que soient la taille de votre structure, son histoire et son évolution, vous pouvez ainsi déployer, en quelques jours, des moyens de protection et de surveillance reconnus et primés au niveau international :

- Le SIEM eGambit sans limite d'événements par seconde ou de débit sur les logs, fourni avec des centaines de règles de corrélations : Windows, UNIX, firewalls…
- L'agent eGambit Endpoint Security qui accompagne votre antivirus sur les serveurs et les stations, pour trouver les vulnérabilités et les menaces furtives et avancées : espionnage, sabotage, rançons…
- Sans parler du NIDS, de nos leurres informatiques (*honeypots*), de l'inventaire, des audits et des technologies de Forensics pour lever des doutes sur de probables compromissions.

Par ailleurs, TEHTRIS, en tant que MSSP, effectue une surveillance continue, avec ses experts, ses robots et ses moteurs d'intelligence artificielle. Les clients reçoivent des certitudes techniques, sans faux positifs, avec les constats, les conséquences, les preuves et les solutions à appliquer, dans l'esprit ISO 27035 avec une traçabilité totale via les tickets du puissant Frontend eGambit.

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

Au niveau des collectivités territoriales, et de manière générale pour le Service Public, nous travaillons avec l'Union des Groupements d'Achats Publics (UGAP) qui intègre notre offre eGambit dans son catalogue. Exemple : protection des réseaux de type grande Métropole française avec eGambit.

De la TPE à la multinationale, en passant par les PME et les ETI, nous offrons le meilleur de eGambit à n'importe quelle taille de structure, avec différentes gammes. Le panel de nos clients s'étend de la TPE d'une ZI jusqu'au CAC 40, avec des activités variées (banques, assurances, industries), de la Chine aux USA, en passant par le Moyen-Orient et l'Europe. eGambit s'impose comme une solution scientifique globale offrant une vision à 360°. ■■■

INFORMATIONS PRATIQUES

→Solution phare
eGambit, cyber arsenal défensif

→Contact
Eléna POINCET, co-CEO
→Téléphone
+33 (0)972 50- 80 33
→Courriel
press@tehtri-security.com
→Web
www.tehtris.com

TEHTRIS

PUBLI INFO

LA SÉCURITÉ N'EST PLUS UN FREIN À LA TRANSFORMATION NUMÉRIQUE

Loïc GUEZO, CyberSecurity Strategist Southern Europe, Trend Micro

Les collectivités locales et les ETI représentent un vecteur de développement très important pour Trend Micro, qui a ainsi opté pour un maillage territorial de ses équipes, au plus près des bassins régionaux. L'éditeur souhaite, de plus, leur apporter le même niveau de protection qu'aux grandes entreprises au travers d'une offre dédiée, de manière à ce que la sécurité ne soit plus un frein pour la transformation numérique de ces dernières.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

Les collectivités locales comme les ETI sont au pied du mur de leur transformation numérique. Cette transformation doit se faire avec les caractéristiques propres de ces organisations. Et sauf erreur de ma part, ou exception qualifiée, la plupart d'entre elles n'ont pas encore la sensibilisation ad hoc quant à la Sécurité de l'Information des nouveaux environnements qui leur sont proposés.

Comment répondent-elles aux questions suivantes :

- Bascule vers le Cloud Public ou des applications métiers « tout en un » SaaS ?
- Migration vers Office 365 ?
- Réseau à plat ?
- Crise suite à un Ransomware ?

Les questions sont nombreuses et les réponses seront souvent orientées par… l'absence (ou pas) d'un responsable SSI dans l'organisation concernée.
Classiquement, il sera un « rôle porté » par un administrateur technique, qui fait au mieux en fonction des budgets alloués, en bout de course, et de la sensibilité de sa Direction Générale ; la variable d'ajustement étant son temps passé à gérer les situations de crise pour remettre tout en ordre, jusqu'à la prochaine crise technique…

Ceux qui s'en sortiront mieux devront avoir réussi à établir une vision stratégique partagée quant à la protection de leur patrimoine informationnel et de leurs systèmes critiques, nécessaires à leur fonctionnement… Vision qui doit se traduire en Gouvernance : budget et moyens humains, mais aussi sponsorship sur la durée de la Direction Générale, au risque de retomber comme un soufflet dans quelques trimestres.

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

Nous avons établi une couverture géographique spécifique pour nos forces commerciales, afin qu'elles soient au plus près des bassins régionaux (Lille, Nantes, Rennes, Toulouse, Grand Est…). Elles sont alors à même de connaître sur la durée les collectivités locales et ETI de notre territoire national. De façon organisationnelle, nous avons depuis plusieurs années maintenant la démarche mise en place récemment par l'ANSSI quant à la couverture régionale des correspondants locaux.

Les collectivités locales et les ETI sont un vecteur de développement commercial très important pour nous, à l'image du potentiel d'emploi qu'elles représentent en France.

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

Une gamme complète orientée ETI permet d'apporter le même niveau de sécurité en mode « Worry Free », c'est-à-dire « prestation de services » sans investissement physique local, complexe à gérer par l'ETI. Une collectivité locale pourra, en fonction de son organisation, besoin, taille… décider d'utiliser cette approche ETI ou l'approche classique de Trend Micro.

Les évolutions de notre gamme sur cette approche ont montré notre sens de l'anticipation des besoins, par exemple dans le secteur de la Santé où nous savons accompagner de toutes petites entités régionales, comme des établissements très demandeurs (tels que les GHT par exemple), en évolution forte due au plan de réorganisation du dispositif national.

La sécurité n'est plus un frein à la transformation numérique. ■■■

INFORMATIONS PRATIQUES

➔Solution phare
Worry-Free Business Security Services

➔Contact
Trend Micro France
➔Téléphone
+33 (0)1 76 68 65 00
➔Courriel
sales@trendmicro.fr
➔Web
www.trendmicro.fr

TREND MICRO™

PUBLI INFO

USERCUBE, LEADER DES SOLUTIONS IAM / IAG EST PLÉBISCITÉ PAR L'UGAP

Christophe GRANGEON,
Directeur Général et Associé de USERCUBE

Alors que l'offre de cyber sécurité ne cesse de s'étoffer, il est frappant de constater à quel point elle est dissonante par rapport au niveau réel de maturité des entreprises. Le « back to basics » de l'ANSSI n'a jamais été aussi vrai. Ainsi, avant d'investir dans des outils avancés, il est urgent de commencer par gérer correctement les utilisateurs et les accès au Système d'Information. USERCUBE propose une solution de gestion des identités sans équivalent sur le marché et une gamme de services de mise en œuvre associés, l'ensemble étant disponible au catalogue UGAP.

GS Mag : Quels sont les principaux enjeux auxquels sont, selon vous, confrontées les collectivités territoriales et les ETI en matière de sécurité numérique ?

Au-delà du bruit de fond médiatique autour de la cyber sécurité, et de quelques attaques qui défient la chronique, il ne faut pas se méprendre. Les enjeux en termes de sécurité numérique pour les ETI et les collectivités restent plutôt basics : il s'agit d'abord de maintenir la continuité d'exploitation et de préserver les secrets fondamentaux. Et n'en déplaise à la myriade de consultants « qui consultent » et en font leur miel, la priorité n'est pas à l'application de la LPM ou de la règlementation européenne sur les données personnelles, mais à la préservation des secrets commerciaux et salariaux. Combien de commerciaux sont passés à la concurrence avec la base clients, la liste des prix, le plan marketing, les propositions en cours ? Et que dire de ceux qui ont toujours accès au CRM et continuent à recevoir leurs mails plusieurs mois après leur départ ? Quid de l'administrateur qui accède aux partages bureautiques de la Direction Générale ou de la Direction des Ressources Humaines ? J'ai en tête l'exemple d'un ami, dirigeant en charge d'une restructuration, qui a trouvé sa fiche de paie affichée un matin à la cafétéria…
A une époque de désengagement massif des collaborateurs et de défiance vis-à-vis de l'entreprise, la sécurité numérique passe d'abord par une parfaite maîtrise des identités et des accès au Système d'Information. C'est d'ailleurs exactement ce que préconise l'ANSSI dans son guide « d'hygiène informatique ».

GS Mag : De quelle manière adressez-vous ces problématiques au sein de votre entreprise ?

La mise en place d'une solution d'administration et de gouvernance des identités et des accès permet de répondre à des questions de base : « Qui accède à quoi ? Ces accès sont-ils légitimes ? Qui les a validés ? ».
Les plateformes traditionnelles de gestion des identités ne sont pas adaptées aux collectivités et ETI. En effet, elles se positionnent très largement comme des solutions de type « boîte à outils » qui nécessitent une grande expertise fonctionnelle et technique, pour le bonheur des consultants et autres intégrateurs, et qui induisent des coûts de mise en œuvre prohibitifs.
A contrario, USERCUBE offre une proposition de valeur de rupture avec une réduction des coûts de mise en œuvre et des délais de déploiement optimisés d'un facteur 3 par rapport aux concurrents. Au-delà des qualités purement techniques, les clients plébiscitent la richesse fonctionnelle de la plateforme Usercube qui permet de couvrir tous les besoins IAM, IAG et Data Governance avec un seul logiciel.
L'offre est disponible en mode « On Premise» et en « SaaS » sur AZURE. Par ailleurs, nous changeons drastiquement les règles du jeu en proposant une mise en œuvre industrielle qui permet de réduire la charge de projet coté client.
Enfin, la solution et les services associés sont disponibles au catalogue UGAP, ce qui est un prérequis pour travailler avec les collectivités. L'Union des Groupements d'Achats Publics (UGAP) est d'ailleurs en train de déployer Usercube pour ses besoins propres.

GS Mag : Comment votre gamme de solutions est-elle amenée à évoluer en ce sens ?

Notre objectif est de continuer à abaisser significativement le TCO des projets en réduisant drastiquement la charge de travail de nos clients et en simplifiant la conduite du changement. En proposant des services orientés « métiers », nous comptons véritablement révolutionner les usages pour toutes les problématiques qui concernent l'identité numérique. ■■■

INFORMATIONS PRATIQUES

→Solution phare
Usercube Identity Governance & Administration Suite

→Contact
Christophe GRANGEON
→Courriel
sales@usercube.com
→Web
www.usercube.com

USERCUBE

INNOVATE **MORE.**

FEAR LESS.

SonicWall peut vous libérer de vos craintes en matière de sécurité informatique afin d'accompagner le développement de votre entreprise. Nous allons au-delà de la simple détection des menaces grâce à une prévention des failles proactive en temps réel qui stoppe les cyberattaques avant même qu'elles ne commencent.

Débridez votre ingéniosité avec SonicWall.

SONICWALL®

Innovate More. Fear Less : Innovez plus. Plus de sérénité.

SonicWall.com : source d'innovation

RANSOMWARE X.

En intégrant des technologies de machine learning à ses mécanismes de détection, la solution **Trend Micro™ XGen™** endpoints security vous protège contre les ransomware et assure l'intégrité de vos données.

Les ransomware ne constituent qu'un volet de de la problématique. Votre faille représentée par ce "X" pourrait aussi être une attaque de type Zero-Day, une menace liée au comportement de vos utilisateurs ou toute activité compromettant l'intégrité de vos données mais aussi votre réputation.

What's your X ?

Trend Micro™ XGen™ endpoints security est LA solution.

TREND MICRO

trendmicro.fr/xgen

#WhatsYourX