CIO.FOCUS

Saisir les opportunités dans les difficultés

EN BREF

Obsolescences techniques, bouleversements réglementaires, pressions des fournisseurs, obligations en termes de responsabilité sociale et environnementale, cyber-attaques... Les problèmes qu'un DSI peut avoir à gérer sont nombreux. Il lui faut bien sûr résoudre les problèmes et réussir à surmonter les défis. Mais les meilleurs DSI sauront trouver dans chacune de ces difficultés une opportunité. A chaque fois, la résolution d'un problème peut être l'occasion de revoir des processus, de former les collaborateurs ou de poursuivre la transformation numérique de l'organisation.
Voici quelques exemples.

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO :
48 rue Cambon 75001 Paris

Rédacteur en chef :
Bertrand Lemaire
blemaire@it-news-info.com
Tél. : +33 (0) 1 41 97 62 10

Principaux associés :
IT Facto et International Data Group Inc.

Président et Directeur de publication :
Nicolas Beaumont

Directeur général : Nicolas Beaumont

CIO est édité par **IT NEWS INFO,**
SAS au capital de 3 000 000 €

Siret : 500034574 00029 RCS Nanterre

SOMMAIRE

© Istock

/ INTERVIEWS

Jean-Claude Laroche (Président, Cigref) : « l'obsolescence artificielle des matériels est un vrai problème »

Le Cigref regroupe 154 grandes organisations françaises utilisatrices d'IT pour un budget IT cumulé supérieur à 50 milliards d'euros par an. Jean-Claude Laroche, son président, prend ici position sur les sujets du moment : l'influence à avoir sur les organes de régulation, la coopération européenne, la sobriété numérique, la cybersécurité, la souveraineté numérique, les relations fournisseurs...

© Thomas Leaud

Jean-Claude Laroche, DSI d'Enedis, a été élu président du Cigref en octobre 2021 après avoir été six ans vice-président.

CIO. Après six ans comme vice-président, vous avez été élu président du Cigref en octobre 2021. Pouvez-vous nous représenter cette association, historiquement, il y a un demi-siècle, « club informatique des grandes entreprises françaises » ?

Jean-Claude Laroche. Le Cigref est une association de grandes entreprises et administrations utilisatrices de solutions numériques. A ce jour, nous avons 154 membres, ce qui représente une communauté de plus de 5000 personnes physiques impliquées individuellement dans nos activités. Un quart des adhérents est constitué d'organismes publics (CNAF, ministères...). En cumul, l'ensemble de nos membres représente un budget numérique annuel supérieur à cinquante milliards d'euros et un effectif de spécialistes IT d'environ 200 000.

Le Cigref a trois vocations. La première est l'appartenance. Le Cigref se veut un lieu d'échange entre responsables et entreprises ayant les mêmes problématiques. Nous voulons aussi être un lieu d'intelligence collective. Nos membres échangent et produisent des réflexions rendues publiques pour enrichir tout le monde, au-delà des adhérents. 89 % des adhérents ont contribué à nos groupes de travail durant la crise sanitaire. Cela draine énormément d'énergie. Enfin, le Cigref a un objectif d'influence. Nous voulons faire valoir les points de vue de nos adhérents devant tous les organes de régulation, non

Jean-Claude Laroche pointe la difficulté de trouver des associations homologues au Cigref dans chaque pays européen.

pas pour défendre un intérêt catégoriel mais avec une vraie préoccupation de défense de l'intérêt général, nos membres étant très variés dans leurs natures.

CIO. Beaucoup de décisions étant prises au niveau européen, le Cigref travaille-t-il avec des associations homologues européennes ?

Jean-Claude Laroche. Tout à fait. Le Cigref a un partenariat étroit avec trois associations homologues : CIO Platform Nederland (Pays-Bas), Voice (Allemagne) et Beltug (Belgique). Les présidents des quatre associations se réunissent une fois par mois. Bernard Duverneuil, mon prédécesseur à la présidence du Cigref, est actuellement vice-président aux affaires européennes. Les travaux et prises de positions en commun ont évidemment un poids plus important au niveau européen, par exemple notre prise de position sur la stratégie de Microsoft et ses impacts négatifs sur la sobriété numérique.

Nous essayons d'étendre ce partenariat à d'autres pays. Des discussions sont en cours avec des associations italiennes et espagnoles. Mais il y a très peu d'associations consacrées au numérique et réunissant des personnes morales en Europe. Nous n'en avons pas trouvé dans chaque pays qui soient à la fois représentatives et actives en matière de production de travaux. Plus fréquemment, il existe des associations de networking de DSI. Or le Cigref, je le rappelle, n'est pas un club de DSI et certains de nos adhérents, tous personnes morales, ne sont d'ailleurs pas représentés en notre sein par leur DSI.

CIO. Et avec d'autres associations non-homologues ?

Jean-Claude Laroche. Depuis très longtemps, nous avons également des échanges constructifs avec des associations complémentaires, y compris celles représentant des fournisseurs. Par exemple, le 9 mars 2022, avec dix autres associations du numérique, nous avons organisé une audition des candidats à l'élection présidentielle autour de six sujets liés au numérique : l'inclusion numérique, la formation et les compétences, l'impact du numérique sur l'économie, l'empreinte environnementale, l'autonomie stratégique nationale ou européenne et enfin la sécurité de l'espace numérique.

Nos travaux avec nos partenaires ne sont pas forcément techniques. Nous avons travaillé sur le licencing avec l'USF (Utilisateurs de SAP Francophones). Avec

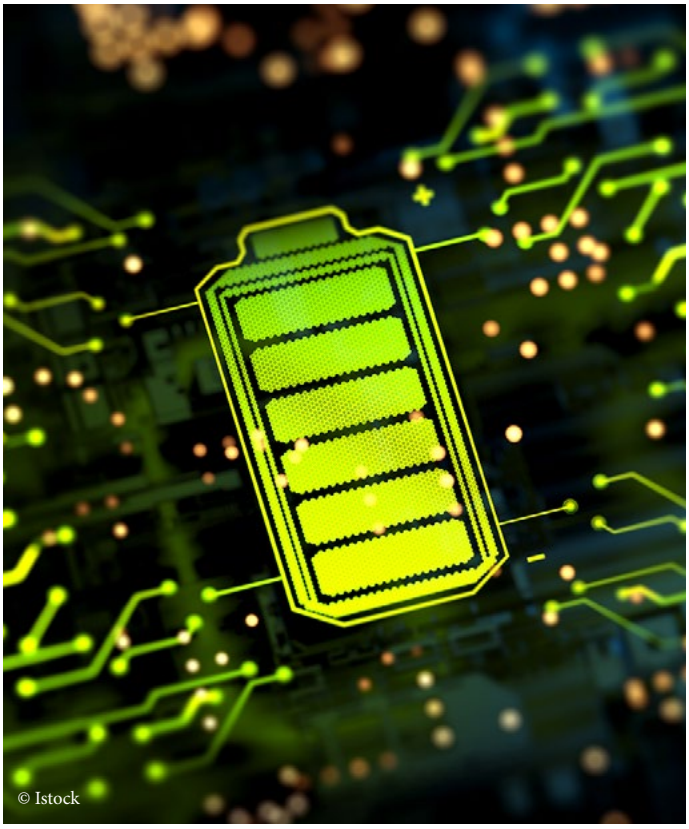
Numeum (syndicat professionnel des fournisseurs IT), nous menons des réflexions sur les liens entre les start-ups et les grandes entreprises ; avec la DFCG sur l'économie du numérique ; etc. Et n'oublions pas notre participation à l'initiative Planet Tech'Care.

CIO. Planet Tech'Care est une initiative sur la réduction de l'empreinte environnementale du numérique et, depuis plusieurs années, le Cigref se veut le héraut de la sobriété numérique. Mais, concrètement, qu'est-ce que cela signifie pour les entreprises utilisatrices ?

Jean-Claude Laroche. Même si le sujet est encore émergent dans les entreprises utilisatrices, il ne s'agit pas de se donner bonne conscience.

Le premier problème, pour avoir une action concrète, est de mesurer l'empreinte environnementale du numérique. Il y a beaucoup de travaux sur le sujet et il commence à y avoir des convergences, un consensus. Ainsi, on peut dire que 70 % de l'empreinte environnementale du numérique sont liés à la production et à la distribution des équipements, 20 % au fonctionnement des datacenters (cloud inclus) et des réseaux ainsi que, enfin, 10 % aux usages effectifs en entreprises. Alors, certes, tout ce qui concerne les e-mails et autres usages sur les terminaux, au coeur d'un certain nombre de discours, cela a certes un impact mais mineur.

La première chose à faire, c'est par conséquent de prolonger la durée de vie des équipements (PC, smartphones, serveurs...). L'obsolescence artificielle des matériels est un vrai problème. En particulier, l'obsolescence provoquée par les montées de version des logiciels : les éditeurs ne doivent pas forcer à une évolution du matériel, d'où notre position en octobre 2021 critiquant le fait qu'un passage à Windows 11 peut entraîner une obsolescence matérielle. L'impact est potentiellement considérable pour les grandes entreprises si cela les conduit à accélérer le renouvellement de leur parc, à savoir des dizaines de milliers de postes. L'obsolescence du matériel est, pour nous, un véritable cheval de bataille. D'autant que cela gêne aussi le réemploi de machines déclassées, par


© Istock

exemple données à des associations, et l'économie circulaire. Pour réduire le coût environnemental, notamment en eau, de la fabrication des composants, il faudrait aussi pouvoir mieux recycler les matériels en fin de vie. Nous sommes conscients que si on multiplie la durée de vie du matériel par deux, l'activité des constructeurs est évidemment divisée par deux, mais cette évolution s'impose compte tenu du contexte environnemental. Or nous avons été en sens inverse depuis des années.

Concernant plus directement les utilisateurs (donc nos membres), il faut parler de l'empreinte environnementale des projets. Numériser un processus a certes un coût pour l'environnement mais cela peut remplacer une manière de faire antérieure plus impactante. La question est donc bien la mesure de la valeur d'un projet numérique non seulement sur le plan économique mais aussi en matière de RSE. La notion de business case doit être étendue.

Par ailleurs, quand, dans un projet, on crée du code, il faut l'optimiser (taille du code, consommation en mémoire...). Mieux le code est écrit, moins il a un impact environnemental élevé et plus il est fiable donc plus le système est résilient. Dans chaque projet, il ne faut jamais négliger la question de la résilience.

Au-delà des projets, dans le fonctionnement au quotidien des systèmes d'information, il y a par exemple de nombreuses techniques d'optimisation des datacenters (réglage fin de la fourchette de températures acceptables pour leur fonctionnement, amélioration de leur climatisation...).

Le Cigref peut produire des méthodes, soutenir des initiatives, pousser à appliquer de bonnes pratiques mais la réglementation a un rôle irremplaçable. Il faut notamment obtenir la publication des données environnementales de la part des fournisseurs et intégrer ces données aux critères d'appels d'offres.

CIO. L'environnement n'est pas votre seul combat. La cybersécurité fait partie de vos grandes préoccupations, y compris en matière de sensibilisation, par exemple avec la campagne Hack Academy en 2015. Concrètement, qu'est-ce qu'un DSI peut faire ?

Jean-Claude Laroche. Jadis, on caractérisait la cybersécurité avec une approche en gestion de risques. Aujourd'hui, les attaques ont lieu partout, ce n'est plus une menace ou un risque mais bien une réalité et une confrontation permanente. Les cyber-attaques connaissent une très forte croissance en sophistication comme en nombre. L'ANSSI a ainsi rappelé que les intrusions avérées se sont accrues de 37 % entre 2020 et 2021. C'est pourquoi, en 2019, le Cigref a soutenu l'Appel de Paris pour la confiance et la sécurité dans le cyberespace.

> *« Face aux cybermenaces, les organisations publiques et privées membres du Cigref ont réalisé de gros efforts pour améliorer leur sécurité.*

Face aux cybermenaces, les organisations publiques et privées membres du Cigref ont réalisé de gros efforts pour améliorer leur sécurité. Elles ont mis en place des dispositifs pour poursuivre l'activité même en cas d'attaque. Dans les grands groupes, l'affaire Saint-Gobain a permis de débloquer des investissements sérieux. A l'inverse, les PME, les centres hospitaliers et les collectivités locales sont nettement plus fragiles.

En 2020, nous avions écrit au Premier ministre pour souligner que le danger était majeur malgré les efforts déjà consentis. En 2021, nous avons soutenu une doctrine en quatre piliers. D'abord, il s'agit de renforcer la sécurité des systèmes d'information. Si le niveau d'investissement s'est accru dans les grandes entreprises, ce n'est pas encore le cas ailleurs. Ensuite, il faut mieux lutter contre la cybercriminalité. Les moyens de la police et de la justice, en la matière, sont très insuffisants et une action diplomatique s'impose pour que les cybercriminels ne puissent pas se cacher dans des pays qui aujourd'hui les laissent faire. Les politiques devraient s'en saisir comme d'un sujet majeur. En troisième pilier, il faut intensifier la cyberdéfense en profondeur. Le sujet est approfondi par d'autres organisations que le Cigref, et il s'agit bien d'un problème régalien : quand on a repéré des acteurs malveillants, il faut pouvoir les neutraliser et le Cigref est par principe hostile au hack-back [« pirater les pirates » en se faisant justice soi-même, NDLR]. Enfin, il faut une régulation européenne pour accroître la sécurité par conception (« security by design »). Quand on achète un jouet à ses enfants, il existe des quantités de normes pour en garantir la sécurité. Mais il n'existe rien de similaire en matière de cybersécurité. Il existe des certifications de haut niveau pour certains produits sensibles mais c'est à peu près tout. L'Union Européenne mène actuellement des consultations en vue d'un prochain Cyber Resilience Act. Si les quatre piliers ne sont pas mis en oeuvre, les problèmes vont aller en s'aggravant. Et la digitalisation de l'économie en sera menacée.

CIO. Après l'environnement et la cybersécurité, vous vous intéressez aussi la souveraineté numérique. Vous appuyez ainsi l'initiative Gaia-X. Quelle est votre approche de la question ?

Jean-Claude Laroche. Côté Cigref, nous n'utilisons pas l'expression « souveraineté numérique ». La souveraineté est en effet un attribut des états et concerne donc les actions des états. De plus, nos adhérents ont souvent une présence mondiale avec

Empreinte environnementale, cybersécurité et confiance dans les fournisseurs sont des sujets majeurs pour Jean-Claude Laroche.

des SI ayant une dépendance forte envers des acteurs eux-mêmes mondialisés. Votre PC est fabriqué en Chine, avec des composants conçus aux Etats-Unis, avec un système d'exploitation américain, tout comme la bureautique.

Le Cigref souhaite seulement que les DSI puissent réaliser leur métier en maîtrisant leur destin et en protégeant les données sensibles. La question se pose surtout dans le cloud. Il faut, selon nous, surtout établir des règles et créer un référentiel de cloud de confiance. Concrètement, qu'est-ce que cela signifie ? D'abord, c'est une relation contractuelle transparente (contrat clair, facturation de la consommation réelle...). Deuxièmement, la cybersécurité doit être de bon niveau. Ensuite, nous voulons être protégés des autorités étrangères. L'extraterritorialité des lois est un problème et, si l'on parle beaucoup du Cloud Act, l'article 702 du Foreign Intelligence Surveillance Act (Fisa) est bien pire et constitue d'ailleurs la base des arrêts Schrems. En aucun cas, un juge américain ne doit avoir accès à nos données.

Les initiatives de type Bleu (co-entreprise Capgemini et Orange), même si elles utilisent des technologies Microsoft, vont dans le bon sens. Bien entendu, si nous pouvions disposer de solutions européennes, nous y serions très favorables.
En fait, la question est pour nous plus celle de la confiance que celle de la souveraineté. Et la compétitivité des acteurs français et européens est une des dimensions du problème.

Il faudrait aussi voir plus loin que le cloud et reprendre la main sur les composants [point aussi soulevé par Nicolas Fournier, DGNUM du Ministère des Armées, NDLR] comme sur les solutions proposées aujourd'hui par les grands éditeurs. Pour construire ces solutions européennes, la question des ressources humaines est critique.

Enfin, sur la souveraineté, un point récent est à prendre en compte : dans les très grands groupes, on utilise l'harmonisation des systèmes d'information pour unifier les fonctionnements à une maille mondiale. Mais, avec le cloud, les conflits géopolitiques impactent les DSI. Par exemple, si l'on a une présence en Russie et si les Etats-Unis y coupent le cloud, la filiale locale qui utilisent des outils Saas américains peut y perdre son système d'information ! Récemment, certains membres se sont aussi posés la question de changer leurs solutions de sécurité s'ils utilisaient celles de Kaspersky. La nationalité du fournisseur devient de ce fait un problème émergent.

CIO. Sur le sujet des fournisseurs, vous disposez de plusieurs groupes de travail. La relation entre les organisations utilisatrices de technologies et les grands fournisseurs est-elle toujours aussi catastrophique ?

Jean-Claude Laroche. Ces groupes de travail sont très utiles car ils permettent de mettre en relation nos membres et les dirigeants des fournisseurs. Nous avons besoin de nous parler parce que nous avons des intérêts contradictoires et nous avons besoin de bien comprendre les stratégies, les roadmaps, les tarifs, etc de nos fournisseurs. Les confinements nous ont pénalisé parce qu'ils n'ont pas simplifié les contacts. Dans ces échanges, le Cigref porte les intérêts de ses membres. Nous exprimons d'ailleurs volontiers nos désaccords. Même si chaque membre du Cigref achète parfois pour plusieurs dizaines de millions d'euros de produits aux grands fournisseurs, nous restons individuellement des petits clients pour certains

acteurs mondiaux, et nous gagnons à nous regrouper. Nous devons lutter contre des abus de position dominantes sur ces marchés oligopolistiques. Le problème se pose évidemment sur la bureautique mais pas seulement.

CIO. Certaines fonctions transverses (comptabilité, paye...) ne sont pas sources d'avantage compétitif et on pourrait imaginer que les entreprises mutualisent leurs efforts pour développer et maintenir des solutions open-source. C'est ce que fait l'Adullact pour les collectivités locales. Pourquoi cela n'a-t-il pas lieu ?

Jean-Claude Laroche. Je ne crois pas à la scission entre SI transverses et métiers en termes de création de valeur. Par exemple, pour un ERP, soit on migre avec une vision purement technique et un coût net, soit on profite de cette migration pour revoir les fonctionnements et dégager de la performance. C'est d'autant plus vrai que la numérisation des processus trouble les frontières. Où sont les référentiels de données ? Dans les SI métiers ou dans les ERP ? C'est très variable selon les entreprises. Donc, oui, nous sommes à la merci d'éditeurs qui font ce qui n'est en aucun cas notre métier mais qui est au coeur de nos métiers.

Dans ce contexte, nous cherchons des relations contractuelles équilibrées et à garantir le bon fonctionnement du marché.

CIO. L'actualité des deux dernières années, avec la crise sanitaire, a montré l'importance du système d'information dans le fonctionnement des entreprises. Le Covid-19, de ce fait, a-t-il été le Grand Soir des DSI ?

Jean-Claude Laroche. Non mais, sans aucun doute, la crise sanitaire a constitué un accélérateur de la prise de conscience de la place des systèmes d'information dans nos organisations. Les DSI qui ont pu faire face ont bénéficié d'une vraie estime en retour. Depuis la crise sanitaire, quand ce n'était pas encore le cas, le DSI n'est plus une fonction support mais au centre du jeu.

La pandémie a été un tournant qui a amené de nouvelles manières de fonctionner, bien sûr en entreprises mais pas seulement. Cela a été aussi le cas, par exemple, dans les écoles. Et on a ainsi pu constater l'ampleur du problème de l'inclusion numérique tant le numérique a pris un poids important. Dans le même temps, chacun a aussi pu prendre conscience de l'importance du contact humain.

Cela étant dit, les entreprises ont vécu la crise sanitaire de manières très différentes. La logistique alimentaire ou les centres hospitaliers ont eu une activité démultipliée tandis que, à l'inverse, le transport s'est effondré. Dans les secteurs en surchauffe, les DSI ont dû faire face dans un contexte difficile. Dans les secteurs en effondrement, il a fallu que les DSI préparent l'après-crise dans un contexte beaucoup moins porteur.

Globalement, la crise a amené une croissance du nombre de projets numériques. L'IT est devenue une bouée de sauvetage et a obtenu un rôle encore plus central.

CIO. Quelles grandes tendances voyez-vous à l'IT dans les prochains mois et années ?

Jean-Claude Laroche. Je vous renvoie bien sûr à notre Rapport d'orientation stratégique présenté lors de notre assemblée générale 2021. Nous y avons étudié les enjeux technologiques face aux nouveaux usages, les risques IT liés aux cybermenaces comme aux questions géopolitiques, les nouvelles formes de travail, les questions environnementales...

Nous avons ainsi défini des scénarios types pour l'avenir, du monde régulé au far west. Des groupes de travail ont ensuite été créés pour nous préparer à chacun des scénarios évoqués.

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO

/ INTERVIEWS

Véronique Puche, DSI de la Cnav : « le RGCU et le DRM représentent une mine d'or de données »

Entrée en 2009 à la Cnav (Caisse nationale d'assurance vieillesse) comme responsable du domaine MOA action sociale, Véronique Puche a d'abord occupé des fonctions de maîtrise d'ouvrage, dont la direction entre 2015 et 2018, avant de devenir directrice des systèmes d'information en mars 2018. Dans cette interview, elle évoque les grands chantiers en cours, dont le RGCU et le DRM, ainsi que les grandes orientations du SI de la Cnav.

© Istock

© Bruno Lévy

Véronique Puche, DSI de la Cnav, a notamment accompagné la mise en place du RGCU (répertoire de gestion des carrières uniques), un référentiel gérant plusieurs milliards de données.

CIO. Pour commencer, pouvez-vous nous présenter le rôle de la Cnav au sein de la sphère sociale et ses principales missions ?

Véronique Puche. La Caisse nationale d'assurance vieillesse (Cnav) est un organisme public de droit privé. Elle gère le réseau de l'assurance retraite, qui correspond à la branche retraite du régime général de la Sécurité sociale. Ce réseau compte 15 caisses d'assurance retraite et de la santé au travail (Carsat), 4 caisses générales de sécurité sociale (CGSS) en outre-mer et une caisse de sécurité sociale à Mayotte. La Cnav couvre les salariés, mais aussi les travailleurs indépendants depuis la fin du RSI.

Notre mission principale est de verser les retraites et d'assurer le suivi des paiements, ainsi que tout le travail de préparation en amont. Il s'agit notamment de récupérer tous les éléments de carrière afin d'évaluer les droits à prestation. Nous avons également des missions d'action sociale, visant à aider les publics les plus fragilisés dans le cadre d'actions inter-régimes.

L'assurance retraite compte environ 21 millions de cotisants et couvre près de 15 millions de retraités. En 2020, elle a versé 132,6 milliards de prestations.

CIO. Dans ce contexte, quels sont les grands clients de la DSI de la Cnav ?

Véronique Puche. Nous travaillons pour trois catégories d'utilisateurs. D'abord, les collaborateurs de la Cnav, à qui nous mettons à disposition des postes de travail, des outils de collaboration et des applications de gestion métier, par exemple pour la maîtrise des risques, la traçabilité des actions, etc. Nous travaillons également pour les assurés. En back-office, nous fournissons les outils qui permettent de suivre les carrières et de délivrer les paiements. Nous avons aussi développé une offre de services adaptée aux attentes des assurés, notamment sur lassuranceretraite.fr, avec des services en ligne pour toutes les catégories, actifs comme retraités. En 2020, le site a dépassé les 70 millions de visiteurs et 430 000 demandes de retraites en ligne ont été enregistrées en 2021. Enfin, nous travaillons pour nos différents partenaires, notamment les autres organismes de la sphère sociale et les autres régimes de retraite. Nous avons environ 200 partenaires, auprès desquels nous avons une mission d'opérateur, et nous échangeons près d'1,5 million de fichiers avec eux sur un an.

CIO. Et quelles sont les grandes briques du système d'information retraite ?

Véronique Puche. Au niveau fonctionnel, les grandes briques concernent la gestion des carrières, le processus de liquidation des droits, qui gère le calcul et le versement des pensions, ainsi que la relation client, aussi bien avec les agents de la branche retraite que les assurés sur le front. D'autres composants gèrent la dématérialisation des flux entrants et sortants, les activités et les demandes.

Nous gérons aussi plusieurs référentiels, dont le répertoire de gestion des carrières uniques (RGCU). Le plus ancien est le système de gestion des identifications (SNGI), qui date de 1988.

Enfin, nous travaillons aussi avec plusieurs grands éditeurs, notamment Microsoft et Oracle. Nous avons aussi une solution de Pegasystems pour l'outillage de Syrca. Sur nos métiers support, nous avons mis en place SAP pour la partie budgétaire et comptable avec le projet Sinergi, et notre SIRH est sur HR Access.

CIO. Pour gérer tous ces éléments, comment est organisée la DSI de la Cnav ? Avez-vous quelques chiffres sur ses activités ?

Véronique Puche. La DSI de la Cnav compte environ 1 300 collaborateurs, répartis sur l'ensemble du réseau de l'assurance retraite. Nous avons aussi des équipes régionales de proximité dans les Carsat. Nous gérons environ 24 500 postes de travail dont 18 000 portables, 7 000 serveurs, 7500 machines virtuelles déployées sur 500 serveurs physiques et plus de 2 000 bases de données, et nous faisons en moyenne 680 mises en production par an.

CIO. Quelles sont les principales missions de la DSI à l'heure actuelle ?

Véronique Puche. En interne, la DSI conduit un programme de transformation profonde du système d'information de la Cnav, avec plusieurs enjeux parfois un peu concurrents. Nous travaillons notamment sur la modernisation des infrastructures et la refonte de plusieurs briques fonctionnelles. Fin 2021, nous avons lancé une étude pour notre prochain schéma directeur. Il faut savoir que la Cnav fait l'objet d'une COG (convention d'objectifs et de gestion) permettant de déterminer l'ensemble de ses engagements. Actuellement, nous sommes dans la période charnière pour préparer la future COG. Côté IT, nous établissons un schéma directeur des systèmes d'information (SDSI), un chantier que nous menons parallèlement à la COG. Le SDSI est lié à celle-ci, mais il a une portée plus large, car nous travaillons aussi sur des missions opérateurs pour les partenaires.

> *« Il faut savoir que la Cnav fait l'objet d'une COG (convention d'objectifs et de gestion) permettant de déterminer l'ensemble de ses engagements.*

En parallèle, nous devons en effet contribuer à la co-construction du SI retraite inter-régimes et interbranches. Selon les projets, nous pouvons être un organisme contributeur, utilisateur ou opérateur. Le

Véronique Puche, DSI de la Cnav : « Selon les projets, nous pouvons être un organisme contributeur, utilisateur ou opérateur. »

but est d'avoir un SI interbranches le plus mutualisé possible. Dans ce cadre, nous sommes opérateurs d'un certain nombre de référentiels, en intervenant sur l'ensemble des champs. Par exemple, nous avons construit le RGCU, en assurant sa conception et son développement, mais aussi l'hébergement, l'exploitation et l'administration. Nous avons aussi un portail commun inter-régimes avec le GIP (groupement d'intérêt public) Union retraite et nous développons également une offre de services en ligne pour l'ensemble des 42 régimes. Nous participons aussi au développement d'une API « Sécu » pour qu'elle expose de plus en plus de données.

Nous travaillons aussi sur le « bien vieillir », afin de délivrer les prestations et de gérer l'évolution des services en ligne. Nous venons par exemple de mettre en production un service pour demander l'allocation personnalisée d'autonomie (APA).

Enfin, nous assurons également tout le maintien en conditions opérationnelles des systèmes d'information. Nous devons faire tout ceci plus vite, mieux et à un coût maîtrisé, ce qui est l'équation impossible de toute DSI.

CIO. Pouvez-vous nous détailler les transformations que vous avez mises en oeuvre sur les infrastructures ?

Véronique Puche. Au niveau des infrastructures, nous nous sommes attaqués à deux grands défis. D'abord, nous avons souhaité réduire le nombre de nos datacenters, pour des raisons à la fois économiques et de développement durable. Cette démarche a demandé deux ans de préparation. En avril 2021, nous avons achevé une première opération sensible de consolidation sur notre site de Tours, où nous avons rapatrié les environnements de production qui étaient sur notre datacenter de Lyon. Ensuite, en cible avant l'été 2022, nous concentrons nos environnements de travail (développement de projets, qualification...) sur le site de Lyon. Ainsi, les environnements complets de production sont à Tours et ceux de travail à Lyon. Nous avons également un troisième datacenter de secours sur un autre site, pour garantir un rétablissement des applications en 2 heures à 6 heures ouvrées sans aucune perte de données. Nous gérons des données sensibles avec de gros volumes, il est donc essentiel d'avoir une infrastructure de secours.

Le second défi était de mutualiser l'ensemble des infrastructures régionales. Cela représente un important chantier de transformation. Nous avons mis en place la V1 d'un cloud privé en interne, afin de pouvoir proposer différents services en fonction des usages. Nous mettons à disposition l'ensemble des services à travers un catalogue et des workflows, pour les délivrer aux équipes de la fonction SI au niveau national et régional. Ce cloud nous apporte aussi un haut niveau d'industrialisation et d'automatisation sur l'ensemble des environnements. Nous pouvons ainsi donner plus d'autonomie aux collaborateurs de la DSI. Le cloud nous permet également d'avoir des indicateurs pour mesurer la consommation des ressources, ce qui nous aide à affiner notre modèle de coûts. Enfin, il fournit un haut niveau de sécurité, conforme aux exigences réglementaires.

CIO. Parmi les gros chantiers menés par la Cnav figure la mise en place du RGCU. Pouvez-vous nous présenter ce projet et nous expliquer son déroulement ?

Véronique Puche. Le RGCU est notre plus grand référentiel, instauré par la loi du 9 novembre 2010, qui a confié à la Cnav sa réalisation, sa construction, son hébergement et son exploitation. Sa cible est de contenir l'ensemble des carrières et d'être alimenté par l'ensemble des régimes de base, mais aussi les régimes complémentaires, ajoutés en 2014. Les données viennent de la DSN. Le but est la mutualisation de ces données, en vue de remplacer 42 bases par une seule. Il s'agit d'avoir la vision la plus complète et détaillée de la carrière de chaque assuré, depuis le premier emploi jusqu'à la retraite.

Nous avons travaillé le modèle de données pour avoir toutes les informations qui permettent de déterminer toutes les règles applicables. Chaque régime pourra y avoir accès. Cela a représenté un énorme défi de structurer les données et de centraliser l'ensemble des flux, avec des problématiques d'alimentation et de restitution des données. Sur ce référentiel, nous avons aussi une approche d'amélioration continue et des enjeux d'intégrité des données, même si sur ce point nous partageons la responsabilité avec les autres régimes.

Nous travaillons dessus depuis 2010 et le RGCU est en production depuis le 1er juillet 2019. Le premier régime à basculer, en mode pilote, a été celui des employés et clercs de notaire, puis nous avons migré l'ensemble des données du régime général (SNGC) en mai 2020, soit six milliards de données, en plein confinement, sans aucune intervention physique. Cela a été un vrai exploit, réalisé par des équipes entièrement à distance. Ensuite, en mai 2021, nous avons migré les données de l'Agirc-Arrco, puis fin 2021 celles de la MSA (Mutualité sociale agricole). Début 2022 s'y sont ajoutées les données des travailleurs indépendants. Il nous reste encore plusieurs petits régimes à migrer, avec un plan de migration étalé sur plusieurs années. Nous avons également un chantier de stabilisation en cours sur la performance et la restitution des données.

Ce projet a représenté 220 000 jours-hommes. Sur toutes les étapes, nous nous sommes fait accompagner par des prestataires. L'Agirc-Arrco est également intervenu, avec un rôle d'opérateur de qualification. La direction du pilotage est à la Cnav, et nous avons des comités de pilotage avec la DSS qui suit le sujet de très près. Le ROI d'un tel projet, qui a coûté 220 millions d'euros, n'est pas immédiatement perceptible, mais celui-ci représente une mine d'or de données pour le futur, avec des perspectives de croisements avec d'autres bases très prometteuses, par exemple pour lutter contre le non-recours ou la fraude.

CIO. Vous avez travaillé avec le GIP MDS (modernisation des déclarations sociales) sur plusieurs sujets, dont la mise en place de la DSN (déclaration sociale nominative). Quel est votre rôle à ce niveau ?

Véronique Puche. Nous travaillons pour deux GIP, le GIP Union retraite et le GIP MDS. Sur les travaux opérés avec ce dernier GIP, nous travaillions sur les DADS, mais avec le remplacement par la DSN, le GIP MDS assure la maîtrise d'ouvrage. Il est également chargé de la relation avec les déclarants. La Cnav intervient comme opérateur pour réaliser le cahier technique de la norme. Nous fournissons au bloc 1 opéré par l'Urssaf caisse nationale un module de contrôle des DSN, et nous réalisons, hébergeons et exploitons le


© Istock

bloc 3, qui stocke les DSN, contrôle les NIR (numéros d'inscription au répertoire Insee, qui sont les numéros de sécurité sociale) et redistribue l'ensemble des données à l'ensemble des régimes de base obligatoires. Nous-mêmes sommes aussi destinataires de ces informations en tant qu'organisme de protection sociale. En janvier 2023, il est prévu d'intégrer les DSN de la fonction publique.

CIO. Un autre chantier important concerne le dispositif de ressources mensuelles (DRM). Pouvez-vous nous le présenter ?

Véronique Puche. Le DRM contient lui aussi beaucoup de données. Il permet de réunir dans une seule base l'ensemble des données de prestations et d'avoir l'ensemble des revenus en un seul endroit. Il a été mis en place en septembre 2019, à l'occasion du projet de réforme des aides au logement. La CNAF et la MSA sont les premiers clients, mais nous l'étendons. C'est une brique clef, qui a permis par exemple de verser en 3 mois les indemnités d'inflation pour les retraités sans re-solliciter les assurés.

Le DRM est alimenté par la DSN et les flux Pasrau (prélèvement à la source sur les revenus autres) mis en place avec le prélèvement à la source. Nous travaillons aussi avec la direction des impôts. C'est la première fois que nous croisons des données sociales et fiscales, c'est une forme de barrière qui tombe.

CIO. Mener de tels projets à bien suppose un certain nombre de prérequis, à la fois techniques et organisationnels. Comment abordez-vous ces aspects ?

Véronique Puche. La Cnav gère aujourd'hui plus de 12 milliards d'éléments de ressources et 6 milliards d'éléments de carrière. Nous avons une stratégie big data afin d'avoir des infrastructures qui peuvent accueillir de tels volumes. En 2018, nous avons redéfini notre socle technique et en 2019 nous avons mis en place une plateforme big data Hadoop, dont la première alimentation a eu lieu en 2021. Nous allons bientôt faire le bilan de cette première phase et préparer le schéma directeur sur ces sujets.

De tels projets nécessitent aussi un certain nombre de révolutions. La première concerne l'organisation et les ressources humaines. Nous avons mis en place une entité dédiée au sein de la DSI, avec une soixantaine de personnes qui disposent de nouvelles expertises sur la data, comme des urbanistes, des architectes et développeurs spécialisés. Une autre révolution porte sur la gouvernance, avec un chantier à la fois en interne et au niveau interbranches, afin de garantir la bonne compréhension et le bon usage des données.

> « *De tels projets nécessitent aussi un certain nombre de révolutions.*

CIO. Quels sont les premiers usages de ces données, notamment au sein de la Cnav ?

Véronique Puche. Les premiers clients qui ont une appétence forte pour ces données, ce sont les services de statistiques, comme notre direction statistiques et prospective, mais nous voulons élargir les usages à l'ensemble des directions métiers, notamment sur la performance, en leur offrant des tableaux de bord et des outils d'aide à la décision, par exemple pour la lutte contre la fraude et le non-recours. Nous voulons aussi étudier de nouveaux usages d'exploration et d'exploitation des données, en utilisant de l'intelligence artificielle pour prédire le comportement des assurés, afin d'avoir une offre de services la plus précise possible.

Véronique Puche, DSI de la Cnav : « Nous voulons étudier de nouveaux usages d'exploration des données. »

CIO. Vous gérez des données très sensibles. Quelles sont les grandes lignes de votre politique de cybersécurité ?

Véronique Puche. Sur la sécurité des données, nous avons mis en place un système d'information avec plusieurs niveaux de contrôle et des dispositifs pour assurer la fiabilité. Nous avons des experts en sécurité pour protéger notre SI, avec un SOC (security operations center) et des SIEM (security information & event management). Nous réalisons aussi des campagnes de sensibilisation auprès de l'ensemble des collaborateurs de la branche retraite. Comme beaucoup d'organisations, nous avons observé une hausse des tentatives d'attaques durant la crise sanitaire, donc nous sommes particulièrement vigilants.

CIO. Quels sont les sujets qui vont se poursuivre sur le prochain SDSI et ceux à venir ?

Véronique Puche. Dans le SDSI qui s'achève, nous avons posé les premières briques de notre transformation, comme le RGCU, mais nous avons également travaillé sur le système d'information qui va les utiliser. C'est le cas par exemple du projet Syrca, un outil pour opérer l'ensemble des régularisations de carrière. Nous sommes en train de finaliser un service de « coproduction » afin qu'un assuré puisse identifier s'il constate des périodes manquantes ou des descriptifs erronés, et qu'il puisse transmettre les informations justes directement au RGCU.

Pour le prochain SDSI, en cours d'élaboration, nous avons notamment des sujets sur le cloud. Aujourd'hui nous avons notre cloud privé en V1 et nous utilisons aussi quelques services de cloud public, comme Office 365 pour la messagerie et les outils collaboratifs, ou notre chatbot Aria, destiné aux usagers du système retraite, qui est hébergé sur Azure. Nous avons donc un modèle hybride et nous étudions les futures options pour le prochain SDSI. Nous menons également des travaux exploratoires avec la direction de la Sécurité sociale (DSS) et les autres caisses nationales sur l'idée d'un cloud Sécu.

La transformation de notre système d'information


© Istock

liquidation est également en cours, avec un premier palier de refonte sur la partie liquidation et paiement. C'est une chaîne de paiements solide, mais qui a trente ans, d'où la refonte. Ensuite, nous menons un ensemble de transformations sur les autres briques : les flux entrants, la dématérialisation, l'archivage, la relation client, les activités... Tous ces chantiers sont déjà cadrés et vont se poursuivre.

> *« Notre nouveau service de prise de rendez-vous en ligne permet aux assurés de trouver un rendez-vous en moins de trois minutes, en physique, en visioconférence ou par téléphone en fonction de l'urgence.*

Nous travaillons aussi sur l'évolution de notre offre de services en ligne. Nous avons récemment mis en place un nouveau service de prise de rendez-vous en ligne, dont l'objectif est de permettre aux assurés de trouver un rendez-vous en moins de trois minutes. Le rendez-vous peut être en physique, en visioconférence ou par téléphone en fonction de l'urgence. Grâce à la géolocalisation, il propose le lieu le plus proche de l'assuré pour les rendez-vous physiques. Depuis mars, 90 000 rendez-vous ont déjà été pris via ce service. Nous allons en faire un premier bilan cet été.

Nous avons enfin des sujets plus techniques, comme de réduire et de maîtriser durablement notre dette IT, à la fois sur le plan technique, technologique et fonctionnel. C'est un chantier que nous avons engagé il y a deux ans. Nous voulons continuer de réduire la dette de façon significative et de la maîtriser durablement.

CIO. Pour finir, qu'est-ce qui vous plaît et vous motive dans votre fonction de DSI ?

Véronique Puche. DSI est une fonction extrêmement transverse, nous avons donc une vision assez large et complète de l'organisation et des processus métiers. Le système d'information est un levier très stratégique : sans SI, il n'y a pas de réforme des retraites possible. C'est un levier pour mettre en oeuvre des politiques publiques.

Ce que j'apprécie dans le métier de DSI, c'est le périmètre très vaste. Tous les jours sont différents ! Il y a un côté « mode pompier » en permanence, mais j'aime travailler dans cette configuration. Dans l'IT il faut être très imaginatif. La dimension technologique avec un grand nombre de machines, de grands volumes de données me plaît également. J'apprécie aussi de travailler avec les informaticiennes et informaticiens, l'un des défis étant d'ailleurs d'avoir un nombre plus important de femmes dans la DSI. Enfin, pour moi travailler pour le service public était impératif.

À LIRE ÉGALEMENT

Élisabeth Humbert-Bottin (DG du GIP-MDS) : « la donnée issue de la paie devient la référence unique »
(cio-online.com)

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Rédactrice-en-chef adjointe

© Istock

/ INTERVIEWS

Frédéric Leconte (DSI de l'Afnor) : « personne n'est à l'abri d'une cyber-attaque »

Le DSI de l'Afnor (Association française de normalisation), Frédéric Leconte, revient ici sur l'incident de sécurité du 18 février 2021, son déroulé, sa gestion et les leçons tirées. Au-delà, il détaille également sa stratégie pour le SI de la structure exerçant la mission de service public de normalisation en France et assurant aussi de la certification, de l'édition et de la formation.

© Bruno Lévy

Frédéric Leconte, DSI de l'Afnor, est revenu sur l'incident du 18 février 2021 et ses suites.

CIO. Pour commencer, pouvez-vous nous représenter l'Afnor et ses métiers ?

Frédéric Leconte. L'Association française de normalisation (Afnor), comme son nom l'indique, est une association loi 1901 exerçant depuis 1926 une mission d'intérêt général d'organisation de la normalisation en France. La volonté du pouvoir politique de normaliser au plan national est plus ancienne que cela. L'unification des poids et mesures, la convention du mètre au moment de la Révolution française s'inscrivent déjà dans cette logique. Idem pour les pratiques et responsabilités des structures ordinales et autres guildes. Actuellement, bien sûr, la normalisation s'inscrit dans un cadre largement international.

Aujourd'hui, l'Afnor a quatre métiers. La normalisation reste notre métier historique. De manière connexe, nous menons de la certification (anciennement mission de l'Afaq avant la fusion avec l'Afnor). Nous éditons les normes, des réglementations, de la documentation... Enfin, nous avons une activité de formation.

Si notre coeur d'activité est en France, nous avons 39 points de présence hors du territoire national pour nos activités hors normalisation. L'association elle-même s'occupe de la normalisation et de l'édition. Les deux autres activités et un certain nombre de points de présence à l'étranger reposent sur des filiales.

Frédéric Leconte peut se réjouir d'une vraie prise de conscience des collaborateurs.

CIO. Du coup, comment est organisée la DSI et le SI ?

Frédéric Leconte. En tant que DSI, je pilote la totalité du système d'information de toutes les entités en France et la DSI France met à disposition des entités à l'étranger des applications métier.

Nous disposons bien entendu d'un « core SI » avec un ERP, des applicatifs RH, etc. A cela s'ajoute un « SI » par métier, c'est à dire un ensemble d'applicatifs dédiés. L'essentiel est on premise, même si nous utilisons quelques SaaS (webconférence, gestion de notes de frais, micro-messaging...).

Les applicatifs métiers résultent en principe de développements maison, éventuellement autour de progiciels. Par exemple, la gestion des normes est construite autour d'une GED car nous n'avions aucun intérêt à reconstruire un moteur de workflow en tant que tel.

Côté bureautique, nous utilisons les versions on premise de Microsoft Exchange et Microsoft Office.

CIO. Le choix de ne pas déployer Office365 est-il lié aux instructions de la Direction Interministérielle du Numérique (Dinum) ?

Frédéric Leconte. Nous sommes une association loi 1901 et ne sommes donc pas destinataires des instructions de la Dinum.

CIO. Le jeudi 18 février 2021, l'Afnor a rencontré un incident grave de cybersécurité. Que s'est-il passé exactement ?

Frédéric Leconte. J'étais en vacances à la montagne et j'ai reçu un SMS à huit heures du matin indiquant que des fichiers étaient chiffrés sur les serveurs et sur des postes, que les personnels rencontraient des problèmes d'accès, etc. J'ai immédiatement appelé le responsable de la production et mon directeur général. Nous avons convenu de diffuser immédiatement un ordre impératif d'arrêt total d'utilisation du système d'information de

l'Afnor, y compris les postes de travail. Nous avons aussitôt stoppé les serveurs. Des collaborateurs sont passés dans les étages pour diffuser l'interdiction. Comme nous étions encore en période pandémique, ceux qui étaient en télétravail ont été prévenus par SMS. Nous avons décidé de faire revenir tous les collaborateurs de la DSI dans les locaux pour que nous puissions mettre en place le plan de réponse à incident . Il fallait en effet réagir rapidement. Comment faire pour permettre aux collaborateurs de travailler ? Comment communiquer avec nos collaborateurs, nos clients et nos partenaires ?

Le RSSI a simultanément sollicité notre prestataire Airbus Cybersecurité. Après les vérifications d'usage à distance, deux experts étaient sur site le soir même.

CIO. Qu'avez vous fait pour analyser l'incident et quelles décisions ont alors été prises ?

Frédéric Leconte. Tout était arrêté et les experts ont donc pu travailler sur le diagnostic durant la soirée du jeudi puis sur l'analyse complète le vendredi et le samedi, y compris sur les PC individuels. La porte d'entrée du rançongiciel se situait sur un poste de travail avec un utilisateur ayant cliqué sur un lien d'un courriel d'hameçonnage.

Sans que je puisse vous donner trop de détails, il s'agissait d'un ransomware classique mais dans une nouvelle version inédite, plus contagieuse, qui a d'ailleurs été transmise à l'ANSSI.

CIO. En termes d'organisation, comment l'Afnor a réagi ?

Frédéric Leconte. La gestion de crise a été pilotée directement au niveau du comité exécutif. La DSI s'est bien sûr chargée de l'aspect informatique et chaque métier a géré la crise pour son propre périmètre. Nous communiquions, dans un premier temps, avec les salariés par SMS en utilisant une plate-forme

Il se trouve que, suite aux attentats de Saint-Denis en 2013, nous avions mis en place un site web permanent de gestion de crise. Et j'avais pris l'initiative, quelques mois plus tôt, de sortir ce site de nos infrastructures pour l'installer sur un hébergement externe mutualisé. L'adresse de ce site est précisée sur nos badges professionnels individuels d'accès à nos locaux avec une mention indiquant de consulter ce site en cas d'incident. Rapidement, nous avons donc utilisé ce site pour piloter la crise et communiquer avec nos collaborateurs.

Ensuite, nous avons créé une messagerie provisoire totalement externalisée. Tous les numéros téléphoniques ont été reroutés vers un centre d'appel qui prenait les messages et les transmettait par mails aux personnes concernées. En effet, notre téléphonie, ToIP, était gérée en interne sur nos propres infrastructures. Donc elle était stoppée.

Nous avons également traité en urgence des questions comme le paiement des salaires de la fin du mois en reprenant un fichier télétransmis le mois précédent à notre banque. Face à la crise, nous avions besoin d'une totale mobilisation de tous nos collaborateurs et il était hors de question d'accroître l'angoisse en ayant un retard sur les versements des salaires.

CIO. Comment avez-vous communiqué vers l'extérieur au moment de la crise ?

Frédéric Leconte. Alors que le sujet émergeait, nous avons rapidement communiqué. En retour, nous avons eu beaucoup de manifestations de soutien et de solidarité. Cela nous a fait chaud au coeur.

CIO. Une fois l'urgence traitée, il a fallu remonter le SI. Comment avez-vous procédé ?

Frédéric Leconte. Nous nous sommes appuyés sur les experts qui nous ont accompagné durant toute la crise. Précisons que nos sauvegardes étaient protégées, ce qui nous a évidemment facilité la tâche. Nous avons estimé que les pirates avaient sans doute pu examiner la totalité de notre infrastructure. Nous l'avons donc réarchitecturée pour nous protéger d'une nouvelle attaque.

Ensuite, nous avons remonté le SI, application par application, dans un ordre validé par le comité exécutif et la direction générale. Côté sites web, Afnor.org a pu

être remis en fonctionnement dégradé au bout d'une semaine, avec un processus de diffusion des normes manuel. Là aussi, le remontage a été progressif.

CIO. Dernier aspect de l'après-crise : il faut éviter une répétition. Quelles ont été les mesures prises ?

Frédéric Leconte. Tout d'abord, il faut rappeler que, dans l'absolu, personne n'est à l'abri d'une cyber-attaque. Bien entendu, nous avons mis en place un SOC, déployé un EDR…

Nous avons aussi mis en oeuvre une série de communications auprès des collaborateurs pour les sensibiliser aux bonnes pratiques en matière de cybersécurité. Nous lançons régulièrement des opérations de hameçonnage de test. Et nous avons rendu plus sévères les règles des mots de passe.

> *« Nous avons mis en oeuvre une série de communications auprès des collaborateurs pour les sensibiliser aux bonnes pratiques en matière de cybersécurité.*

Depuis l'attaque, nous avons constaté une vraie prise de conscience. Maintenant, il arrive que des collaborateurs nous amènent leur PC s'ils ont un doute sur quelque chose (un mail, un incident…). Auparavant, cela n'arrivait jamais. C'est bien sûr beaucoup plus sain.

Enfin, nous avons entamé une démarche de certification ISO 27001. Cette démarche est le couronnement des travaux antérieurs, en assurant ainsi une validation et une valorisation. Lors des premiers contrôles, très peu de non-conformités ont été relevées.

CIO. Au delà de cette crise, quels sont vos autres défis actuellement ?

Frédéric Leconte. Nous poursuivons actuellement la digitalisation du SI de la normalisation avec, en objectif, les « normes du futur ». Il s'agit de diffuser les normes en format XML voire sous forme d'API pour accélérer l'intégration des normes dans le système d'information des entreprises. Dès aujourd'hui, la vente de normes en format papier est tout à fait épisodique.

Côté formations et certifications, nous avons à rendre le parcours le plus fluide possible. Et, bien entendu, nous nous devons d'accroître les formations en mode distanciel.

La certification des entreprises est réalisée par des auditeurs et ceux-ci bénéficient déjà depuis longtemps d'une application qui accompagne la rédaction du rapport final. Bien sûr, il s'agit de poursuivre l'évolution de celle-ci.

CIO. Et côté infrastructures ?

Frédéric Leconte. Nous sommes en ce moment en train de migrer notre datacenter vers l'hyperconvergence. Nous procédons progressivement.

Notre téléphonie est actuellement hébergée sur nos infrastructures et est donc bloquée si le SI rencontre un problème. De plus, elle est un peu ancienne. Nous avons donc lancé un appel d'offres qui est toujours en cours. L'objectif serait d'éviter que, en cas de nouvelle attaque, tous nos outils soient atteints. Il s'agit de répartir les risques pour assurer notre résilience.

Notre plus grand engagement post-attaque a été de nous investir dans la rédaction d'un guide pour aider les entreprises qui vivront cette situation à faire face. Ce document, que l'on appelle chez nous AFNOR Spec, a vocation à recenser les bonnes pratiques utilisées par les structures victimes de cyberattaques, afin d'assurer une continuité d'activité. L'objectif est de partager de l'expertise et des savoir-faire pour contribuer à améliorer la résilience collective aux cyberattaques.

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO


© Istock

/ PROJETS

Decathlon éprouve sa sécurité par un bug bounty

Decathlon a fait tester son site e-commerce tunisien par des hackers éthiques dans le cadre d'un bug bounty avec YesWeHack lors du FIC. Farid Illikoud, RSSI groupe de Decathlon, revient sur cette expérience qui est le premier bug bounty public mené par le groupe.


© Decathlon

Farid Illikoud, RSSI groupe de Decathlon, considère que les bugs bountys sont complémentaires des audits traditionnels.

Avec 1750 magasins (dont 320 en France) dans 70 pays et un chiffre d'affaires de presque 14 milliards d'euros (un quart en France), Decathlon rassemble plus de 100 000 collaborateurs passionnés par le sport. Ce distributeur spécialisé, dont le siège est dans la métropole lilloise, est contrôlé par l'Association Familiale Mulliez (souvent improprement désignée comme « groupe Auchan ») et a logé dans une filiale dédiée, Decathlon Technology, son IT. Bien entendu, Decathlon possède des sites e-commerce. Et, évidemment, comme toutes les boutiques en ligne, ces sites e-commerce sont l'objet de cyber-attaques fréquentes. Leur sécurisation est donc cruciale. Plusieurs démarches sont menées à cette fin. Farid Illikoud, RSSI groupe de Decathlon, nous a expliqué l'intérêt du bug bounty et comment celui-ci vient s'insérer dans une démarche globale.

Les boutiques en ligne de Decathlon sont de deux types technologiques. Il y a d'une part des sites basés sur un développement propre réalisé en interne, d'autre part des implémentations de Prestashop, un progiciel open-source très courant. « Chaque pays choisit sa technologie et mène son implémentation mais nous avons un objectif d'uniformisation du parcours et de l'expérience client » précise Farid Illikoud. Dans le cas de la Tunisie, il s'agit d'un site basé sur Prestashop avec des personnalisations réalisées par une équipe interne de Decathlon située au Canada. Réalisé récemment, ce site a été choisi pour réaliser un bug bounty public à l'occasion du FIC (Forum international de la cybersécurité) qui a eu lieu à Lille du mardi 7 au jeudi 9 juin 2022. Pour le mener, Decathlon Technology s'est appuyé sur YesWeHack.

Une trentaine d'heures pour trouver sept failles avérées

Farid Illikoud précise : « nous menons des bugs bountys privés depuis deux ans avec YesWeHack mais, cette fois, nous avons voulu faire un bug bounty public. » YesWeHack propose, dans le cadre des bugs bountys privés, un ensemble d'une dizaine à une quinzaine de hackers éthiques, avec un roulement d'une opération à l'autre pour profiter d'une variété de compétences. Dans le cas d'un bug bounty public, le nombre de hackers éthiques est plus important : 85 pour celui-ci. Si Prestashop est un progiciel open-source très connu, courant et déjà bien sécurisé, l'implémentation elle-même est à tester, ainsi que des API de connexion au SI, la brique d'identification, etc.

Au total, le bug bounty du FIC a duré une trentaine d'heures à compter du mercredi 8 juin à 10h. Les hackers éthiques engagés dans le bug bounty ont remonté 26 suspicions de failles, 7 se sont révélées avérées. Les équipes sécurité, de développement et de production prennent à chaque fois contact avec le hacker faisant un signalement pour comprendre exactement de quoi il s'agit et vérifier si la faille est avérée. En ce cas, il faut bien comprendre le cheminement du potentiel pirate. « Chaque faille avérée a été trouvée par plusieurs hackers sans concertation » souligne Farid Illikoud. Cette concordance n'est pas une surprise et est même très fréquente dans un bug bounty.

Une correction des failles au fur et à mesure

Les équipes DevSecOps de Decathlon étaient mobilisées sur le FIC durant le bug bounty. Farid Illikoud indique : « nos équipes ont un contrat de SLA interne qui prévoit des délais de correction pour les failles et, lors de ce bug bounty, les corrections ont été réalisées dans la foulée des signalements. Le principal problème d'un bug bounty, c'est de vérifier que les failles signalées sont avérées. » Comme pour tout bug bounty, le principe est celui d'une rémunération du découvreur d'une faille. En l'occurrence, les primes allaient de 500 euros à 5000 euros selon la criticité du problème relevé. La récompense moyenne sur ce bug bounty a été de 1100 euros. « YesWeHack sert d'intermédiaire dans tous les échanges et Decathlon n'a donc aucune information sur l'identité ou le profil des hackers éthiques » relève Farid Illikoud.

Comme il y a une récompense, l'objectif est de tester un environnement déjà sécurisé par des méthodes classiques. Pour Farid Illikoud, « il ne faut pas opposer l'audit et le bug bounty, les deux sont complémentaires. L'audit coûte beaucoup plus cher qu'un bug bounty mais on ne trouve pas les mêmes choses. » L'audit se passe en mode « white box », c'est à dire que l'auditeur a un accès complet au système, un compte pour ce faire et regarde en profondeur le code. A l'inverse, le bug bounty est en mode « black box », c'est à dire que personne ne sait ce que vont tenter les hackers et ceux-ci n'ont pas d'accès privilégié. Ils se comportent comme des pirates.

Audit et bug bounty sont complémentaires

Avant une mise en production, il va de soi que Decathlon réalise un audit, des tests de sécurité et des tests d'intrusion. Les audits sont réalisés par des entreprises spécialisées, avec deux ou trois consultants durant deux ou trois jours. Le bug bounty mobilise bien plus de personnes et permet donc des tests plus nombreux. « L'effet d'exposition amène bien plus de hackers et on trouve forcément plus de choses » se réjouit Farid Illikoud.

Mener l'audit puis un bug bounty permet de cumuler deux types de recherches de failles. L'audit doit bien sûr être réalisé en premier, pour éviter une multiplication de découvertes de failles à rémunérer. Le bug bounty va, lui, avoir une approche similaire à un vrai pirate et sanctionne donc l'effectivité de la sécurisation réalisée avec l'audit.

SUR LE MÊME SUJET

- 13 Mai 2022 : Jérôme Dubreuil (CDO, Decathlon) : « Decathlon est un monde de données »
- 17 Juin 2022 : Mélisa Wiro (gouvernance data Decathlon) : « Nous avons décentralisé la gouvernance des données auprès des métiers. »

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO

© Istock

/ PROJETS

Voies Navigables de France centre son SI renouvelé sur les données

Depuis la réforme de 2013, Voies Navigables de France mène un chantier de refonte de son SI en le centrant sur les données grâce aux outils InterSystems.

© VNF

Benoît Hollebecq, adjoint au DSIN et responsable transformation numérique de VNF, a détaillé la réorganisation de l'établissement public et les conséquences IT.

Historiquement, les voies navigables étaient, en France, gérées par sept agences territoriales à raison d'une par bassin, et une direction nationale de coordination. En 2013, une réforme a abouti à la création d'un établissement public administratif unique, baptisé Voies Navigables de France (VNF), avec sept directions territoriales. VNF assure plusieurs missions. La première est bien sûr d'assurer la navigabilité des voies pour tous leurs usagers (fret, passagers ou loisirs). VNF exploite au quotidien les 6700 kilomètres de voies (canaux, fleuves, rivières...) et les 4000 ouvrages d'art (écluses, digues, barrages...) avec perception des redevances de transport de marchandises et les vignettes pour la plaisance. L'établissement dispose aussi de 40 000 hectares de terrains avec éventuellement des bâtiments (maisons éclusières...) parfois concédés ou loués. Enfin, en liaison avec les agences de l'eau, dont l'objet est la gestion et la protection des ressources en eau, VNF contribue à la gestion de l'eau au-delà de la seule garantie de niveau pour la navigabilité des voies (barrages, bassins de rétention...).

La réforme de 2013 mais aussi les changements d'attentes de la part du gouvernement comme du public vis-à-vis de VNF aboutissent à des nécessités de refonte IT. « Avec la réforme, l'établissement national est passé brutalement de 300 à 4000 agents » observe Benoît Hollebecq, adjoint au DSIN et responsable transformation numérique de VNF. Surtout, chaque établissement régional possédait ses propres systèmes. Chaque DSI créait des applicatifs


© Istock

pour couvrir chaque besoin et par établissement, en plus des systèmes support (comptabilité, GRH...). Au niveau infrastructures, chaque agence territoriale et l'établissement national avaient leur propre datacenter. VNF dispose donc aujourd'hui d'un datacenter national et de sept datacenters régionaux. Benoît Hollebecq pointe : « nous avons dû travailler sur l'urbanisation du SI et aussi sur des référentiels communs (bateaux, collaborateurs, etc.) dans le cadre d'une démarche de Master Data Management avec un gros enjeu d'accessibilité et de gestion des accès à ces référentiels, d'où notre recours à InterSystems. »

Unifier un SI historique éclaté

D'une manière générale, VNF a une volonté de consolidation et de centralisation. Les huit datacenters devraient donc être regroupés, éventuellement sous forme de recours à du cloud externe sous réserve du respect des obligations en termes de fiabilité, de disponibilité et de sécurité. Les référentiels communs ont, eux, été construits dans une base de données verticale avec la solution Informatica. Pour assurer la circulation des données entre systèmes, y compris avec les référentiels, VNF a choisi de s'appuyer sur l'ETL proposé par InterSystems. « Ces chantiers sont longs car il s'agit d'unifier des SI historiques au travers d'une refonte » souligne Benoît Hollebecq.

Une nouvelle étape a été franchie il y a trois ans. Le contrat d'objectifs et de performance signé avec le ministère de tutelle visait alors à dynamiser le transport fluvial. A cette occasion, un plan de modernisation de VNF a été conçu, avec un plan de financement sur plusieurs années. Cette modernisation a évidemment une dimension informatique, en particulier ce qui est nommé « informatique industrielle » par VNF. Cette informatique métier était traditionnellement répartie dans les différentes agences de terrain. Surtout, VNF s'est engagé dans une démarche d'automatisation de ses ouvrages.

Consolidation, modernisation et automatisation

Le maniement des ouvrages et équipements comme les écluses ou les vannes est aujourd'hui encore très manuel. Parfois, certains peuvent être télécommandés. Benoît Hollebecq indique : « nous

sommes en train de mettre en oeuvre des postes de commandes centralisés (PCC) qui vont prendre la main sur la gestion des ouvrages et le pilotage des circulations sur les axes fluviaux ». Cela passe aussi par la multiplication des remontées d'informations par une multitudes de capteurs (caméras vidéos, capteurs de niveaux d'eau, géolocalisation des bateaux...). Les PCC sont actuellement en cours de construction, que ce soit en tant que bâtiments comme d'IT. Un des effets de ce développement de l'automatisation et de l'informatisation a été la création, en Avril 2020, d'une authentique DSIN (direction du système d'information et du numérique), représentée au comité exécutif, en lieu et place d'un simple service informatique.

> *« Nous sommes en train de mettre en oeuvre des postes de commandes centralisés (PCC) qui vont prendre la main sur la gestion des ouvrages et le pilotage des circulations sur les axes fluviaux. »*

Côté applicatifs, la même logique générale de consolidation et de modernisation s'applique. Les multiples applicatifs régionaux sont donc progressivement remplacés et uniformisés. Au niveau des données, les PCC doivent pouvoir collecter toutes les informations issues du terrain, notamment par IoT, et les afficher de manière compréhensible pour les gestionnaires d'infrastructures navigables. Le rôle du datahub Iris d'InterSystems est, pour cela, évidemment central. « Nous sommes aussi en train d'expérimenter le recours à l'IA pour prévoir la disponibilité des voies et des quais afin de fluidifier le trafic » stipule Benoît Hollebecq.

Développer des services nouveaux

Au delà de la consolidation et de la modernisation, très techniques et peu visibles directement par les usagers, l'informatique unifiée va faciliter la mise en place de nouveaux services. Par exemple, aujourd'hui, il n'existe que quelques bornes eau-électricité le long du réseau de voies pour que les bateaux puissent se ravitailler avec des cartes pré-payées. Demain, le nombre de bornes va être démultiplié et, surtout, les usagers pourront les réserver et payer les prestations en ligne ou via une application mobile. De la même façon, les mariniers déclarent en ligne leur itinéraire et le tonnages transportés mais... c'est du pur déclaratif ! Avec des recoupements d'informations et la géolocalisation des bateaux, VNF pourra améliorer la circulation et éviter les encombrements.

La transformation du SI, pour permettre ces nouveautés, reposent sur le passage d'une logique par applicatifs à une logique par services rendus. Techniquement, cela suppose de mettre au centre de l'architecture les données (approche datacentric) et de faciliter les échanges entre applications via des API. La plate-forme d'échange de données sous InterSystems permet aussi de faire le lien entre les anciens outils et les nouveaux, plus digitaux, au fur et à mesure des remplacements. Les agents de terrain commencent à voir les effets de cette transformation en cours : un millier de smartphones a été distribué avec des applicatifs métier mais aussi RH sur un portail de service. Mais Benoît Hollebecq reconnaît : « nous sommes encore au milieu du chemin ! »

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO