N°52

échanges

la performance en revue

DOSSIER

CYBERSÉCURITÉ ET QUALITÉ

GRAND TÉMOIN

SABINE ROUX DE BÉZIEUX,
PRÉSIDENTE DE LA FONDATION DE LA MER

ENSEIGNEMENT

#ETUDIERENAVEYRON : QUALITÉ, SÉCURITÉ, ENVIRONNEMENT AU SEIN DE CAMPUS XIIE AVENUE

Qualite Performance

MAGAZINE D'INFORMATION DU PORTAIL DE LA QUALITÉ ET DE LA PERFORMANCE

ÉDITO

Par Pierre GIRAULT
Président de France Qualité

Focus sur la résilience connectée

Le présent numéro de votre revue Échanges est pour une bonne part consacré aux enjeux et implications de la cybersécurité. Un thème de notre temps s'il en est !

Car depuis quelques années, nombre d'organisations se révèlent confrontées à des attaques de hackers, ciblages de données, perturbations de systèmes, coupures de réseaux, demandes de rançons. Il s'agit parfois d'activités d'espionnage industriel, souvent d'actions de malveillance délictueuse, voire d'accompagnements d'engagement militaire. Avec à la clé des impacts éventuels significatifs, au niveau de l'utilisation de fichiers clients ou du fonctionnement d'applications informatiques par exemple. Très clairement, l'omniprésence des technologies de l'information et de la communication, les capacités quasiment infinies d'interconnexion et d'échanges de data, à la fois permettent beaucoup de facilitations de la vie au quotidien, et exposent les organismes ou citoyens à des dangers potentiels.

Voilà la raison d'être des multiples textes, mécanismes, formations, réflexions, qui portent sur la protection des personnes et des actifs, matériels et immatériels.

Mais en quoi sommes-nous concernés en tant qu'acteurs Qualité ? Suivent trois éléments de réponse.

Qui dit travail sur la cybersécurité dit besoin de structuration des approches, d'assise méthodologique. Justement, différents outils Qualité facilitent le déploiement de dispositifs appropriés autant que le traitement de situations dégradées : analyse des processus et des supports techniques ou numériques associés ; contrôles et audits en matière d'accessibilité et d'intégrité des documents/data de référence ; partage des bonnes pratiques et formalisation de plans de continuité d'exploitation ; Retour d'EXpérience sinon gestion de crise. Notons en outre qu'une certification s'avère envisageable selon la norme ISO 27001, centrée sur le système de management de la sécurité de l'information.

Lire la suite page 4...

échanges

Éditée par : France Qualité • AFQP -- **ISSN** 2679-6600
Directeur de la publication : Pierre Girault -- **Coordinateur :** Michel Cam
Comité de rédaction / lecture : Cécile Arroyo, Bernard Bousaada, Michel Cam, Gérard Cappelli, Laurence Chavanon, Jérôme Cury, Delphine Foucher, Martial Godard, Lise Harribey, Thomas Lejeune, Lucien Penalba, Melissa Rey, Hélène Schmidt
Chef de rubrique Grands Témoignages : Marie Cornet-Ashby
Web : contact@francequalite.fr - www.qualiteperformance.org

FRANCE QUALITÉ

sommaire

Poursuivez la lecture sur
www.qualiteperformance.org

ÉDITO

Suite de l'édito

Deuxième élément de réponse : notre communauté de professionnels, les équipes Qualité de manière générale, ont vocation à assurer de plus en plus le pilotage des démarches d'amélioration continue des performances comme de maîtrise des risques, au sein des organismes publics et privés. Oui, c'est le sens de la Nouvelle Qualité... globale - et oui, c'est l'enseignement majeur tiré de la toute récente enquête-baromètre de la performance, réalisée à grande échelle via le Cabinet international Pyx4, partenaire de l'AFQP. Et les méthodologies éprouvées de prévention, résilience, valent bien entendu pour le risque inhérent à la sécurité digitale, soit l'un de ceux sinon celui à prioriser désormais !

Reste une troisième considération, largement évoquée lors de la Journée française de la Qualité du 23 mai dernier... les démarches de progrès et de prévention apparaissent également comme le ciment d'une dynamique collective/ouverte/citoyenne RSE, comme le fondement d'une consolidation de liens avec l'écosystème, comme le moteur d'une intégration filière ou secteur économique. Y compris et a fortiori à cet égard, la protection cyber est par construction, par nature, le vecteur au cœur de l'ensemble des problématiques partagées par une entreprise avec ses sous-traitants, la supply chain, des entités en interface = c'est au fond le langage, la langue, du dialogue opérationnel.

Bonnes découverte et lecture.

DOSSIER :
Cybersécurité et Qualité

contexte

Cybersécurité, de quoi parle-t-on ?

Par Lisa BOSSU, Référente Nationale Maîtrise des risques de France Qualité, Responsable Qualité du Centre Hospitalier National d'Ophtalmologie des Quinze-Vingts

QU'EST-CE QUE LA CYBERSÉCURITÉ ?

La cybersécurité, également appelée sécurité informatique ou sécurité des systèmes d'information, permet de protéger tous objets connectés via Internet, les serveurs, les applications, les systèmes électroniques, les réseaux et les données, contre toutes attaques malveillantes.
Elle se divise en plusieurs catégories :

- La sécurité réseaux concerne la protection du réseau informatique contre les intrus.
- La sécurité des applications protège les logiciels et les appareils connectés contre les menaces ; une application infectée pourrait ouvrir l'accès à vos données.
- La sécurité des informations garantit l'intégrité et la confidentialité des données.
- La sécurité opérationnelle comprend les processus et les décisions liés au traitement et à la protection des données.
- La reprise après sinistre et la continuité des opérations correspondent à la manière dont une structure répond à une attaque de cybersécurité ou tout autre événement causant une perte d'opérations ou de données.
- La formation des utilisateurs finaux : en ne respectant pas les bonnes pratiques de sécurité, tout le monde peut accidentellement introduire un virus dans un système sécurisé. Apprendre aux utilisateurs à supprimer les pièces jointes suspectes et à ne pas brancher de clés USB non identifiées est essentiel pour la sécurité d'une entreprise.

LES DÉBUTS DE LA CYBERSÉCURITÉ

La cybersécurité est devenue omniprésente, tant dans notre vie professionnelle que personnelle.
Les cyberattaques et la cybersécurité ont fait leurs entrées dès les années 1970.
Et c'est dans les années 2000, que la cybersécurité et les cybermenaces sont institutionnalisées.
A partir des années 2010, prenant conscience de l'ampleur des cyberattaques, le gouvernement propose les premières règlementations (RGPD). En effet, une réglementation devenait urgente car les cyberattaques se faisaient à grande échelle, avec des répercussions irréversibles.

LES « PIRATES-TYPE »

Il existe plusieurs types de cyber-pirates : du hacker agissant seul par challenge ou vengeance, au groupe de hackers organisé dont le but est de revendre, d'effacer ou de divulguer des données.

>> Les attaques de masse

Les attaques de masse sont de nos jours très courantes, car elles ont un très faible coût et touchent à grande échelle un large public.
Les attaquants balayent Internet pour trouver des objets connectés non-sécurisés comme des caméras, des tablettes, des smartphones, des systèmes de domotique, etc.
Ils peuvent arriver à créer un « botnet », c'est-à-dire un réseau d'objets connectés compromis, et contrôlés à distance par un pirate.

>> Les ransomwares ou rançongiciels

Le « ransomware » ou « rançongiciel » est une technique d'attaque de cybercriminalité qui consiste à envoyer à la victime un logiciel malveillant qui codifie l'ensemble de ses données et lui demande une rançon en échange d'une clé de déchiffrement.
L'objectif de cette attaque est d'être sur un champ d'action le plus large qui soit, pour avoir un impact sur un large public et récolter le plus d'argent possible.

Comment se diffusent les rançongiciels ?

Les logiciels malveillants de rançonnage se propagent grâce au « phishing » ou à l'approche dite du « hameçonnage ».

Ces techniques consistent à imiter les couleurs d'une institution ou d'une société (banques, service des impôts, Caisse d'Assurance Maladie, Institution, etc…) pour gagner la confiance du destinataire, et faire en sorte qu'il communique des informations personnelles. Au moment-même où l'utilisateur ouvre le fichier, un logiciel est installé sur son poste à son insu. Ce logiciel chiffre une partie ou l'ensemble des données contenues sur l'ordinateur. Si l'utilisateur souhaite récupérer ses données, il devra payer une rançon, d'où le terme de « ransomware » ou « rançongiciel ».

Comment se protéger des rançongiciels ?

Pour se protéger d'un rançongiciel :

1- Sauvegardez régulièrement vos données,
2- Vérifiez la véracité de l'identité des expéditeurs des emails,
3- Soyez vigilant(e) lors des téléchargements de fichier,
4- Utilisez un antivirus à jour,
5- N'ouvrez pas de pièces jointes en cas de doute sur leur légitimité,
6- Ne téléchargez pas sur des plateformes dites « douteuses ».

>> Les attaques ciblées

Les attaques ciblées sont moins courantes, mais font tout autant de ravages auprès des entreprises ou des personnes victimes.

Les modes opératoires sont plus complexes et demandent des compétences spécifiques ou une connaissance particulière de l'entreprise. L'attaquant connaît parfaitement sa victime, via une cartographie précise, et met tout en œuvre pour l'atteindre. Bien souvent, il s'agit d'espionnage pour obtenir une information (espionnage économique ou industriel, politique, etc…). De telles attaques sont appelées APT pour « Advanced Persistent Threat », qui se traduit littéralement par « menace persistante avancée ».

Comment se protéger des attaques ciblées ?

1- Détruire les messages sans réponse,
2- Choisir des mots de passe sécurisés,
3- Ne pas exécuter d'instructions venant d'un inconnu,
4- Toujours effectuer les mises à jour,
5- Ne pas diffuser d'informations personnelles et/ou confidentielles sur Internet.

>> Les malwares

De nos jours, les menaces également appelées « malwares » ne sont plus aussi différenciées qu'auparavant. En effet, ce qui varie est plutôt le comportement de ces virus.

Par exemple un « Cheval de Troie » va généralement embarquer des fonctions de « backdoor » (porte dérobée), lui permettant de maintenir son accès sur le système ou d'embarquer des fonctions de « keylogger » pour enregistrer la caméra ou encore les frappes du clavier effectuées sur le poste.

>> Les rootkits

Des programmes connus sous le nom de « rootkits » s'installent sur votre ordinateur afin de dissimuler une activité sur le système de fichiers (création, lecture, écriture), une activité réseau, ou encore une activité en mémoire (calculs). Un rootkit peut travailler dans l'environnement de l'utilisateur, sans droits particuliers, ou en profondeur dans le système d'exploitation, nécessitant par conséquent des droits d'exécution élevés.

L'installation de ces programmes nécessite que le système soit préalablement compromis (Cheval de Troie, intrusion). Ces programmes modifient les commandes usuelles de l'administrateur, afin de dissimuler toute trace de leur présence.

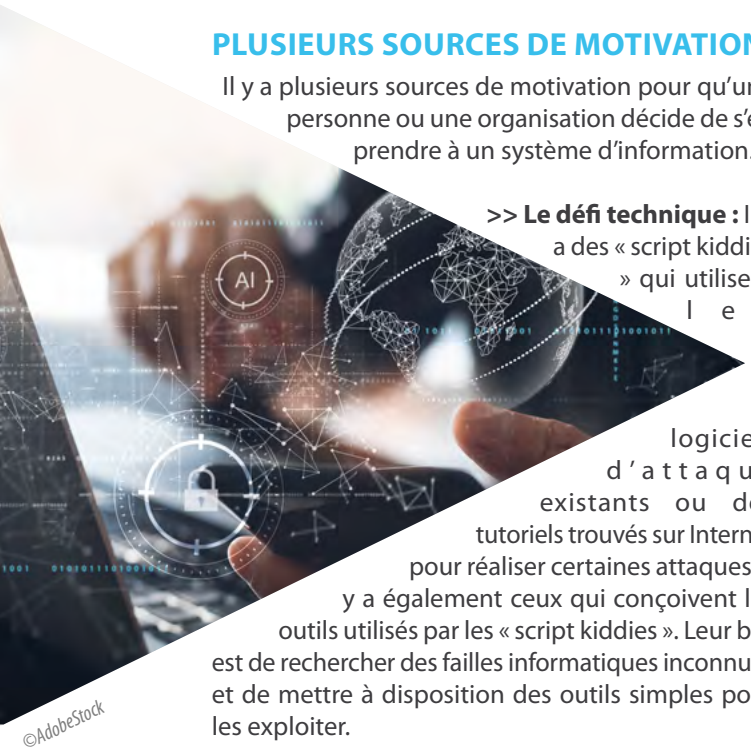
>> Les adwares

D'autres menaces sont moins dangereuses pour vos données à court terme mais tout aussi envahissantes pour votre poste de travail, comme les « adwares » ou les « publiciels ». Ces logiciels publicitaires qui contiennent des programmes utiles, comprennent

également une partie illégitime permettant de vous restituer des publicités ciblées ou non.

PLUSIEURS SOURCES DE MOTIVATION

Il y a plusieurs sources de motivation pour qu'une personne ou une organisation décide de s'en prendre à un système d'information.



©AdobeStock

>> Le défi technique : Il y a des « script kiddies » qui utilisent les logiciels d'attaque existants ou des tutoriels trouvés sur Internet pour réaliser certaines attaques. Il y a également ceux qui conçoivent les outils utilisés par les « script kiddies ». Leur but est de rechercher des failles informatiques inconnues et de mettre à disposition des outils simples pour les exploiter.

>> Les hacktivistes : Au-delà de l'aspect lucratif, certains hacktivistes recherchent l'impact le plus large possible pour avoir un effet de taille critique. Assurément, l'objectif est bien de diffuser un message idéologique et d'influencer l'opinion à travers des attaques informatiques. En général, le niveau technique utilisé alors par les attaquants n'est pas très élaboré. Il s'agit par exemple d'utiliser la défiguration de sites Internet qui ne nécessite pas de niveau technique élevé mais dont l'impact peut être important.

>> L'attaque étatique : Certaines attaques sont dites « étatiques » et se caractérisent généralement par leur aspect très ciblé, leur degré de sophistication et l'utilisation de vulnérabilités inconnues de manière coordonnée. Des lanceurs d'alertes ont ainsi révélé par exemple que certains opérateurs téléphoniques américains livraient chaque jour aux services de renseignements, la totalité des données téléphoniques en leur possession concernant les communications téléphoniques au sein des États-Unis, mais aussi entre les États-Unis et l'étranger.

>> L'espionnage : Les cyberattaques peuvent également servir pour de l'espionnage.
Dans ce cas, les attaquants vont chercher à exfiltrer les informations stratégiques des entreprises et des particuliers comme des secrets de fabrication, des orientations de recherche et de développement, etc. Les secteurs les plus touchés sont l'armement, le spatial et le secteur pharmaceutique.

>> La vengeance : Enfin, il existe une autre catégorie d'attaques ciblées, lorsque l'attaquant est tout simplement par exemple un ancien employé de l'entreprise « victime ».
En effet, les anciens employés connaissent assez bien les systèmes d'information voire les potentielles vulnérabilités. Dans ce cas-là, les motivations de l'action sont d'ordre émotionnel ou centrées sur le fait de tirer profit de la situation.

LES CONSÉQUENCES POUR LES VICTIMES DE CYBERATTAQUES

Pour les entreprises et les particuliers, les conséquences des cyberattaques peuvent être de plusieurs natures :
>> La perte financière : la perte financière engendrée par la cyberattaque est la plus couramment rencontrée.
>> L'atteinte à l'image : au-delà de l'aspect financier, les attaques informatiques peuvent jouer sur l'avenir des dirigeants et/ou de l'entreprise.
Par exemple, lors du piratage d'un site de rencontres extraconjugales, le PDG de la société propriétaire du site a décidé de démissionner, comme suite à la publication de 30 Go de données du site contenant les noms, les comptes utilisateurs, les courriels et les adresses ainsi que les historiques de navigation de ses clients.
Malheureusement, cette expérience a démontré que cela pouvait aller tragiquement plus loin puisque certaines personnes se sont suicidées à la suite des révélations du site.
Il s'agit là d'un aperçu des conséquences sociales, humaines que peut avoir un piratage.

COMMENT SE PRÉMUNIR ?

Quelques règles d'or de sécurité méritent attention, selon les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes Informatiques).
Malheureusement, de nos jours, l'utilisation simple d'un logiciel de sécurité (antivirus, pare-feu, logiciel, applications, etc…) ne suffit plus à se protéger des cyberattaques.
Protéger son cyberespace permet d'éviter des conséquences désastreuses d'une cyberattaque.
En effet, il nous revient de respecter quelques règles de bonnes pratiques telles que décrites dans le guide rédigé par l'ANSSI.

1- Choisir ses mots de passe
Choisir ses mots de passe avec soin. Favoriser une phrase composée de 12 caractères dont au moins 1 majuscule, 1 minuscule, 1 chiffre, 1 caractère spécial. Bien sûr, éviter que cette phrase soit trop évidente. N'écrire aucun mot de passe sur des documents, ne pas en sauvegarder la teneur sur un navigateur. Pour conserver vos différents mots de passe, il existe des coffres-forts de mots de passe.

2- Mettre à jour régulièrement ses logiciels et applications
Mettre à jour régulièrement son matériel et son système informatique (navigateur, antivirus, pare-feu, applications...). Les éditeurs de vos logiciels et applications mettent des correctifs à disposition pour plus de sécurité. Ces mises à jour ne concernent pas uniquement des nouvelles fonctionnalités mais également apportent souvent des correctifs de failles de sécurité. Elles valent pour l'ensemble des objets numériques connectés tels que les ordinateurs, tablettes, télévisions, smartphones, etc...

3- Bien connaître ses utilisateurs et ses prestataires
Pour éviter toute attaque de votre matériel, soyez vigilant(e) avant d'accéder à une adresse Internet (URL), d'installer un logiciel ou d'accéder à toute autre ressource disponible sur un support externe (clé USB, disque dur).
Afin d'éviter le téléchargement ou l'installation de logiciels malveillants, il est nécessaire…
• De sensibiliser les utilisateurs (sur les impacts) ;
• D'utiliser des outils de détection de malwares (antivirus…) ;
• De séparer les droits d'administrateur de ceux des utilisateurs ;
• De télécharger les logiciels sur les sites de leur éditeur ;
• D'utiliser des supports amovibles sains.

4- Effectuer des sauvegardes régulières
Effectuer des sauvegardes régulières et sur différents supports (CD, clé USB, serveur, etc.).
En cas de cyberattaque, ne pas faire de sauvegarde vous expose et expose votre entreprise à de lourds préjudices en cas de perte. En effet, il est primordial de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement sans affecter son activité.
Dans le cas d'une cyberattaque (virus, rançongiciel, etc.) ou d'une erreur humaine (suppression/altération de dossiers-fichiers), il est également nécessaire de pouvoir retrouver les documents disparus.
Pour assurer la continuité de son activité, il est nécessaire d'avoir une politique de sauvegarde régulière des fichiers et applications.

5- Sécuriser son accès Wi-Fi
Le réseau Wi-Fi sans fil est plus vulnérable aux attaques, s'il est mal sécurisé – cf. absence de mot de passe, mot de passe trop simple ou technologie de chiffrement peu sécurisée (WEP).
Pour utiliser une connexion Wi-Fi sécurisée, favoriser la technologie WPA2-PSK avec un mot de passe fort.
Et rester vigilant(e) avec les Wi-Fi publics (hotspots) qui sont proposés dans les bars, hôtels, restaurants, les bibliothèques, les aéroports, etc... Malheureusement, bien souvent ces accès ouverts ne sont pas sécurisés.

©AdobeStock

6- Etre prudent(e) avec son smartphone et/ou sa tablette

Les smartphones et les tablettes sont présents dans nos foyers mais également dans les entreprises. Il est évident que ces objets connectés contiennent des informations confidentielles personnelles et professionnelles. Ce qui est indéniable, c'est que ces objets connectés demeurent très mal protégés. Afin d'éviter les risques pour votre entreprise, pensez à séparer les usages professionnels et personnels en n'utilisant pas vos appareils personnels pour votre travail. Portez une attention toute particulière sur les applications que vous souhaitez installer. En effet, elles peuvent être une source de fuite de données et augmenter la surface d'attaque de votre smartphone/tablette. Installez uniquement les applications qui vous sont réellement utiles.

7- Protéger ses données lors de déplacements

Aujourd'hui, les objets connectés (ordinateurs portables, smartphones, tablettes, caméra, etc…) sont une mine d'or d'informations. De tels – petits - objets sont devenus indispensables dans notre confort de vie. Voyager avec… augmente le risque de menaces sur nos informations sensibles. Il est impératif de protéger ses données lors de chaque déplacement. Car en cas de vol ou de perte, cela peut avoir de lourdes conséquences sur votre vie personnelle ou les activités de l'entreprise.

8- Être prudent(e) lors de l'utilisation de sa messagerie

Evitez d'ouvrir les mails suspects.

Lancez un antivirus avant d'ouvrir les pièces jointes de votre messagerie pour vérifier qu'elles ne contiennent aucun virus connu.

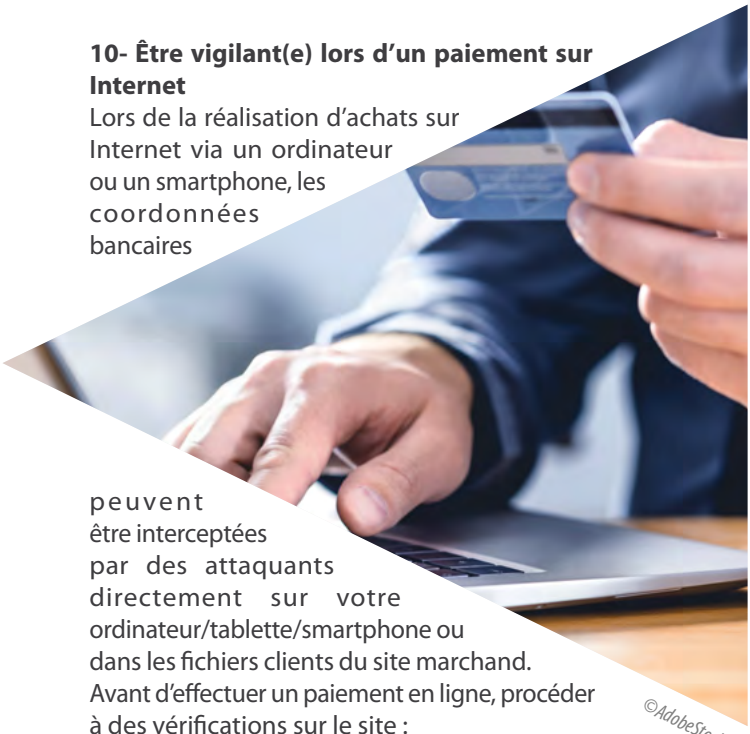
Ne relayez pas de canulars ou de messages de type chaînes de lettres, porte-bonheur, pyramides financières, appel à solidarité, alertes virales, etc.

9- Télécharger ses programmes sur les sites officiels des éditeurs

La plupart des contenus numériques présents sur les sites Internet n'offrent pas de garantie de sécurité sur le site hébergeur. Une fois installés, ces programmes vont permettre à des personnes malveillantes de prendre le contrôle à distance de votre poste. Les hackers pourront alors espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Dans le cadre de votre utilisation professionnelle, l'installation de ces outils est a priori réservée au service informatique de votre entreprise.

10- Être vigilant(e) lors d'un paiement sur Internet



©AdobeStock

Lors de la réalisation d'achats sur Internet via un ordinateur ou un smartphone, les coordonnées bancaires peuvent être interceptées par des attaquants directement sur votre ordinateur/tablette/smartphone ou dans les fichiers clients du site marchand.

Avant d'effectuer un paiement en ligne, procéder à des vérifications sur le site :

- S'assurer que la mention « https:// » apparait bien au début de l'adresse du site Internet.
- Vérifier la légitimité du site Internet en prenant garde aux fautes d'orthographe par exemple (même si cela ne vous garantit pas complètement sa légitimité).
- Vérifier la présence d'un cadenas vert dans la barre d'adresse de votre navigateur.

11- Séparer les usages personnels et professionnels

Séparer les usages personnels des usages professionnels. Cela vous parait évident, mais qui n'a jamais envoyé de mail professionnel via son smartphone personnel ou vice-versa. Or les mesures de sécurité sont très différentes entre les équipements à but personnel et ceux à but professionnel.

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, smartphone, tablette, etc.) dans un contexte professionnel. Cette pratique pose des problèmes, notamment lors de la perte ou du vol d'un équipement, puisque des données d'entreprises potentiellement sensibles y transitent.

Dans ce contexte, il est donc préconisé de :

- Ne pas faire suivre les messages électroniques professionnels sur des services de messagerie personnelle.
- Ne pas héberger de données professionnelles sur les équipements personnels (clé USB, téléphone, etc.)

ou sur des moyens personnels de stockage en ligne.
• Ne pas connecter de supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.
Le non-respect de ces bonnes pratiques offre la possibilité à des personnes malveillantes de voler des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

12- Prendre bien soin de son identité numérique
C'est-à-dire ne jamais transmettre de données personnelles et sensibles, comme des coordonnées bancaires, sur des sites qui ne présentent pas toutes les garanties requises (forums, jeux, sites de téléchargement, etc…).

ETABLIR UNE CHARTE INFORMATIQUE AVEC SES COLLABORATEURS

La sécurité du numérique est l'affaire de tous.
En effet, au sein d'une entreprise, il est important d'établir une stratégie en matière de sécurité des systèmes d'information, avec ses salariés, comme par exemple une charte informatique.

L'objectif de cette charte est d'informer chacun des acteurs de ce qu'il peut faire (bonnes pratiques) ou de ce qu'il doit faire (obligations) pour maîtriser les risques.

La charte peut ainsi prévoir par exemple de verrouiller systématiquement son poste de travail en quittant son bureau durant les pauses et à la fin de la journée de travail, ou encore d'accompagner les visiteurs dans leurs déplacements ou de ranger ses documents confidentiels.


©AdobeStock

analyse

Cybersécurité et Qualité : une alliance de cœur et de raison

Par Patrice THIRIOT, Administrateur du CLUSIR PACA, Club de la Sécurité de l'Information Région Provence-Alpes-Côte d'Azur

Entreprise membre de l'AFQP PACA

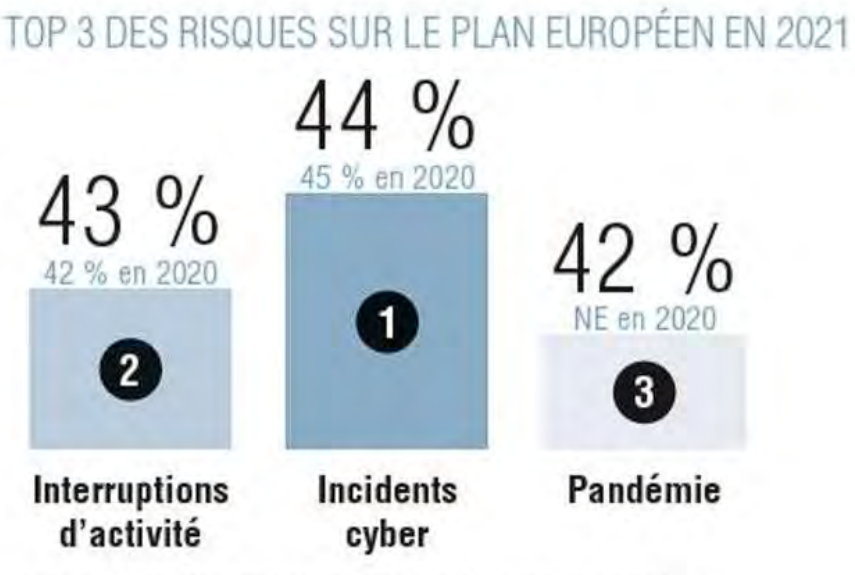
Dans nos sociétés hyperconnectées où les solutions et les offres numériques sont omniprésentes, l'actualité met en lumière très régulièrement les cyberattaques et les maux numériques qui nous affectent, tant dans la sphère professionnelle que personnelle.

Cantonnée il y a encore quelques années aux seuls domaines techniques, la sécurité des usages numériques est aujourd'hui au premier rang des préoccupations des dirigeants tant politiques qu'économiques. Les malveillances numériques concernent les organisations de toutes tailles et tous les domaines d'activité. La prévention et la lutte contre l'insécurité numérique sont aujourd'hui au cœur de la défense des processus d'importance vitale des organisations.

DE LA PROTECTION PHYSIQUE DES INSTALLATIONS À LA PRISE EN COMPTE DES MENACES NUMÉRIQUES

En France, sous la 5ème République la notion de défense des « installations d'importance vitale » apparaît pour la première fois dans une ordonnance du 29 décembre 1958. Centrée sur la prévention du sabotage et donc la seule protection physique des installations dont l'indisponibilité « risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation », cette ordonnance ne concernait également que les seules entreprises désignées par le ministre des armées.

Longtemps focalisés sur les risques de conflits armés ou de terrorisme, les différents dispositifs de défense



Source : Baromètre Allianz des risques 2021 pour les entreprises (1 278 entreprises interrogées dans le monde)

©AdobeStock

nationale et les lois de programmation militaire ont intégré, assez récemment la notion de cybermenaces. En France, c'est seulement en 2008, dans le livre blanc sur la défense et la sécurité nationale, que le risque numérique est mentionné parmi les vecteurs à prendre en compte dans le cadre des politiques de défense nationale.

Au cours de la décennie qui a suivi, la menace cyber n'a cessé de se renforcer dans le domaine professionnel et personnel au rythme de la dématérialisation des activités et de la multiplication des objets connectés qui ont aujourd'hui gagné tous les pans de notre société.

C'est la prise en compte des cybermenaces qui avait conduit en juillet 2009 à la création sous la tutelle du SGDSN de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Sa vocation initiale était de protéger les dispositifs numériques des services de l'État. Le rôle de l'ANSSI s'est progressivement élargi et concerne aujourd'hui la défense des intérêts vitaux de la nation et des services essentiels de la société française, tant privés que publics.

LA CYBERSÉCURITÉ : UNE RECHERCHE DE CONTREPOIDS AUX CYBERMENACES

Par l'effet corrélé de l'accélération de l'enjeu numérique et du développement des cybermenaces, les questions de sécurité numérique échappent aujourd'hui aux seules directions informatiques et s'installent progressivement au sein de la gouvernance élargie et du pilotage global des organisations.

L'ANSSI définit la cybersécurité d'une organisation comme « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. »

Pour mettre en œuvre une politique de sécurité de ses systèmes d'information, chaque organisation doit mener une série de travaux destinés à définir les axes de sa propre politique de cybersécurité. On peut citer notamment la nécessité de :

- Prendre conscience de son patrimoine de données à protéger, des processus et des actifs essentiels au fonctionnement de son entreprise à l'aide de la réalisation d'un inventaire ;
- Déterminer les sources de menaces potentielles et les dépendances aux parties prenantes aussi bien externes qu'internes susceptibles de mettre en difficulté l'entreprise ;
- Cerner et évaluer les cybermenaces et les risques de non-conformité numérique pouvant affecter la bonne marche des activités de l'entreprise ;
- Cartographier et mesurer la criticité des vulnérabilités pouvant affecter les infrastructures, les services et les systèmes d'information de l'entreprise ;
- Traiter les risques de cybersécurité à l'aide de plans d'actions pilotés et mis à jour régulièrement ;
- S'attacher à impliquer par la sensibilisation et la formation tous les collaborateurs dans la chaîne de cybersécurité de l'entreprise ;
- Veiller à évaluer et améliorer de manière itérative et régulière le dispositif de cybersécurité de l'entreprise en fonction de l'évolution des menaces et de l'évolution des métiers de l'organisation.

CYBERSÉCURITÉ ET QUALITÉ : DE FORTES SIMILITUDES DANS LES APPROCHES À MENER ET DES ASSOCIATIONS À RECHERCHER

La normalisation des approches de cybersécurité et de management de la sécurité des systèmes d'information s'est appuyée largement sur les travaux, les pratiques et les normes apparues beaucoup plus tôt dans le domaine du management de la qualité.

Apparue en 2005, la famille des normes de sécurité des systèmes d'information ISO 27000 s'est ainsi inspirée des travaux et des notions de système de management déclinés 18 ans plus tôt dans la famille des normes de qualité ISO 9000.

Ainsi, tout comme les normes de qualité, les normes


©AdobeStock

de sécurité des systèmes d'information poursuivent un objectif commun visant à favoriser la confiance des parties prenantes de l'entreprise.

Publiée en 2005, révisée en 2013 puis tout récemment en 2022, la norme ISO 27001 définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). Ce SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme. L'objectif poursuivi est de protéger les fonctions et informations de toute perte, tout vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique.

Dans les deux familles de normes, on retrouve une démarche d'amélioration continue fondée sur des itérations régulières alliant phase de planification, de déploiement, de contrôle et d'ajustement. Largement inspirée des travaux du statisticien Deming, la norme de sécurité des systèmes d'information ISO 27001 formalise une démarche similaire au PDCA (Plan-Do-Check-Act) mentionné dans la norme de management de la qualité ISO 9001.

Qualiticien, gestionnaire de risques ou responsable de la sécurité des systèmes d'information (RSSI) utilisent ainsi très souvent des boites à outils et des approches communes.

Cette similitude des méthodologies et cette appétence à l'amélioration continue des dispositifs facilitent largement les collaborations et les synergies entre qualiticiens et personnels en charge de la sécurité des systèmes d'information.

On peut ainsi militer pour la mutualisation de certains travaux entre ces deux corps de métiers. En effet, pour une part significative des activités, le partage d'expériences, la transversalité et le décloisonnement des approches entre qualiticien et RSSI favorisent la mise en place de logiques « gagnantes-gagnantes » au service de l'entreprise.

Par exemple, la similitude des politiques et les systèmes de management des démarches servent à la fois la cybersécurité et la qualité des actions portées par les différents métiers de l'organisation. Qualiticien, manager de risques, responsable de la sécurité des systèmes d'information mais également délégué à la protection des données sont autant de relais et de tremplins pour promouvoir l'amélioration continue des pratiques et des activités de l'entreprise mais également de sa cybersécurité.

Il est, en effet, utile de rappeler que :

- La cybersécurité n'est pas uniquement une affaire de spécialistes : pour atteindre son but, elle doit avant tout associer, relayer, impliquer toutes les composantes de l'organisation sur laquelle elle s'applique ;

- La cybersécurité est l'affaire de tous : le niveau de sécurité numérique d'une organisation s'apprécie en effet à la hauteur du maillon le plus faible de la chaîne de sécurité numérique de l'entreprise. La sensibilisation et la formation de tous les collaborateurs de l'organisation sont indispensables pour leur permettre d'acquérir les gestes barrières et les postures d'hygiène numérique adaptées. Au même titre que l'entraînement à des exercices incendie ou d'évacuation de bâtiments, la réalisation régulière d'exercices de crises numériques est également à considérer ;

- L'efficacité et la pertinence d'une politique de sécurité des systèmes d'information se fondent sur une prise de conscience et une évaluation objective des risques numériques pesant sur les activités de l'organisation. Qualiticien et RSSI ont là encore des échanges à organiser pour mettre en œuvre des appréciations pertinentes ;

- Enfin, la cybersécurité tout comme la qualité se fondent sur une démarche prônant l'amélioration continue gouvernée par un système de management permanent et itératif, favorisant la montée en maturité de l'organisation de l'entreprise notamment dans le domaine de la sécurité et de la conformité numérique.

« Qualiticien, gestionnaire de risques ou responsable de la sécurité des systèmes d'information (RSSI) utilisent ainsi très souvent des boites à outils et des approches communes. »

Dans une logique d'appréciation systémique du fonctionnement d'une organisation, il est donc utile de mixer les approches et d'enrichir les évaluations. Outre le fait d'éviter les effets de silos, ces collaborations collégiales entre auditeurs, qualiticiens, RSSI, chefs de projets poursuivent un objectif commun au service de l'amélioration des processus, de la sécurité numérique de l'entreprise et de l'implication de chaque collaborateur.

tendance

L'emploi cybersécurité en hausse

Par Lise HARRIBEY, France Qualité, d'après l'étude Apec « Cybersécurité, un marché de l'emploi cadre diversifié et de plus en plus porteur », publiée en juin 2022

L'Apec vient de publier une étude sur le marché de l'emploi cadre en cybersécurité. Réalisée en partenariat avec le Pôle d'excellence cyber (PEC), cette étude s'inscrit dans le cadre d'un programme de réflexion plus ample, portant sur les enjeux en matière de cybersécurité.

L'étude révèle que « le volume des offres d'emploi cadre exigeant des compétences dans le champ de la cybersécurité a quasiment doublé entre 2017 et 2021, passant de 3 650 à 7 000 offres. Cette augmentation est d'autant plus forte qu'elle est très largement supérieure à l'évolution du nombre d'offres d'emploi cadre publiées au global sur apec.fr au cours de cette même période (+ 20 %). »

Parmi les métiers les plus demandés :
- La conception, le déploiement et la maintenance informatique (Build & Run) 46 %,
- La gouvernance, les risques et la conformité (GRC) 18 %,
- La gestion et la réponse aux incidents 11 %,
- L'audit et l'expertise 11 %,
- Le commercial et le marketing 9 %,
- L'ingénierie généraliste en cybersécurité 5 %.

Pourtant, la cybersécurité est encore un domaine relativement récent, qui souffre d'une méconnaissance de l'ensemble des métiers qu'elle recouvre, freinant les recrutements.

Face à ces constats, les enjeux de demain de la cybersécurité se situent autour de la formation et de l'innovation.

Retrouvez l'intégralité de l'étude à télécharger ci-dessous, plus de 24 pages d'analyse et de prospective sur l'emploi cadre dans ce secteur.

témoignage

La cybersécurité vue par Inkivari

Propos recueillis auprès de Cyril MARCH, Gérant d'Inkivari, par France Qualité

Entreprise membre de l'AFQP Grand-Est

Depuis 2018 et la mise en application du Règlement Général sur la Protection des Données personnelles (RGPD), Inkivari accompagne les entreprises, associations, groupements et toute collectivité dans le pilotage de leur conformité. Inkivari dispose des compétences informatiques, juridiques ainsi que d'un service d'assistance en gestion de projets transverses, dpo@ssist, qu'elle met à disposition de ses clients pour guider leur plan d'action de conformité. Pour les structures concernées par l'obligation de désignation d'un Délégué à la Protection des données (DPO/DPD), Inkivari propose une prestation d'externalisation de cette mission.

Notre volonté est de transformer une démarche de prime abord contraignante (obligation légale) en levier de performance. En prenant en compte les attentes et besoins de nos clients dans le respect de leur organisation et de leurs valeurs, notre méthode s'inscrit dans une stratégie qualitative d'amélioration continue.

France Qualité : Quelle place occupe la cybersécurité au sein de votre entreprise ?

Cyril MARCH : La cybersécurité est un des piliers de la protection des données personnelles, 5 articles du RGPD mentionnent l'obligation de celle-ci ; ce volet est transversal dans la feuille de route de conformité. En phase d'audit, nous examinons les mesures organisationnelles et techniques de sécurité. Une fois les risques résiduels identifiés, nous formulons des conseils et des propositions de mesures correctives. Rappelons qu'en cas de violation de données susceptible d'engendrer un risque pour les droits des personnes physiques, l'entreprise doit le notifier dans les 72 heures à la CNIL, voire à la personne concernée en cas de risque grave (art. 33 et 34 RGPD).

Plus largement, suite à un incident de sécurité, nous accompagnons nos clients dans leur analyse afin de réduire les risques et les récidives. L'ensemble des mesures est structuré dans un registre et le plan d'actions est régulièrement alimenté des procédures et mesures correctives. Nous capitalisons sur ces expériences, pour l'ensemble de nos clients.

France Qualité : Depuis combien de temps vous intéressez-vous à ce sujet ?

Cyril MARCH : J'ai une formation d'ingénieur en informatique, et que ce soit pendant mes études ou à titre plus personnel, concernant les mouvements d'hacking éthique et de Bug Bounty... la lutte contre les vulnérabilités en matière de cybersécurité a été et reste omniprésente. Ce qui m'a convaincu de me lancer dans le RGPD, c'est qu'enfin une loi (enfin un règlement) imposait à tous de se préoccuper de la sécurité des données ! Les données sont partout, toute organisation publique ou privée collecte de la donnée quelles que soient sa taille et sa maturité en matière de sécurité. Il était temps de s'en préoccuper et notamment de mettre en lumière l'importance de la cybersécurité afin de pallier les vulnérabilités menaçant nos données !

France Qualité : Quels sont les enjeux associés à la cybersécurité pour votre entreprise ?

Cyril MARCH : La cybersécurité est un enjeu majeur pour notre entreprise, les risques peuvent être désastreux financièrement, ou encore pour notre image et notre crédibilité envers nos clients. Les « Supply chain attack » peuvent nous prendre pour cible et « rebondir » chez nos clients. Ce type d'attaque est trop souvent méconnu : un fournisseur, sans en être conscient, peut être le « maillon faible » de


©AdobeStock

tout système d'information au sens large. En effet, sans être détenteur de données sensibles, il dispose d'informations plus ou moins directes sur la manière de fonctionner, la gouvernance, les éventuels défauts et des failles de sécurité, en bref des vulnérabilités qu'un cyber-attaquant saura ou tentera d'exploiter. Assurer la sécurité des données que nous traitons est une obligation et une responsabilité à l'égard de nos clients.

La sécurité est une affaire collective face à des attaques de plus en plus massives, ciblées, structurées et techniques. En limitant nos risques, nous limitons ceux de nos clients. Une telle démarche de détection et de gestion des risques est corrélée à la démarche de mise en conformité au RGPD. Lors de l'audit de cartographie des traitements de données à caractère personnel, le DPO peut détecter des anomalies et orienter vers une meilleure maîtrise des process... La mise en oeuvre d'une de stratégie de protection est une réelle opportunité pour nos clients.

« Notre volonté est de transformer une démarche de prime abord contraignante en levier de performance. »

France Qualité : Avez-vous une expérience sur le sujet à relater (cyber-attaque, formation, prévention…) ?

Cyril MARCH : Très récemment, un de nos clients a fait l'objet d'une tentative d'arnaque au RIB. L'interlocuteur « victime » a eu les bons réflexes, et bien que la tentative ait été mise en échec, il a tout de même signalé l'incident de sécurité selon la procédure de déclaration d'incidents mise en oeuvre dans le cadre de la conformité RGPD ; suite à sa déclaration :

- La procédure de vérification des demandes fournisseurs a été renforcée ;
- Une action de sensibilisation des collaborateurs les plus exposés a été menée.

France Qualité : Quels méthodes / outils mettez-vous en place sur le sujet ? Pourquoi, comment ?

Cyril MARCH : La cybersécurité est un sport de longue haleine qui se pratique tous les jours. Comme tout sport, il demande un esprit d'équipe. En effet, la mise en place d'une bonne hygiène cyber suppose de mobiliser l'ensemble des équipes au sein d'une même entreprise. Le facteur humain est trop souvent laissé de côté dans la cybersécurité, or lors de nos audits on détecte fréquemment qu'il s'agit de l'une des plus grosses vulnérabilités et qu'il est donc primordial de maîtriser ce risque. Cette maîtrise passe aussi bien par des ateliers de sensibilisation afin d'informer massivement les équipes des dangers actuels et futurs en matière de cybersécurité, que par des recommandations plus spécifiques faites à nos clients suite à leur demande.

France Qualité : Quels sont vos projets en la matière ?

Cyril MARCH : Nous ouvrons un pôle cyber et nous appuyons sur un réseau d'experts que ce soit en redteam ou blueteam. Ce pôle aura pour but d'offrir une expertise plus complète pour la conformité de nos clients, et ainsi de proposer une vision novatrice et transversale alliant le juridique à la technicité cyber. Inkivari a pour volonté une constante amélioration de ses projets et outils afin de répondre au mieux aux enjeux de demain.

France Qualité : Existe-t-il un lien au sein de votre organisation entre la cybersécurité et la fonction Qualité ? Si oui, lequel ?

Cyril MARCH : Grâce à la transversalité de la mission Qualité, le responsable Qualité est un bon binôme avec le RSSI/DPO. En effet, il permet de lier les mesures organisationnelles du DPO et celles techniques du RSSI tout en respectant la politique générale de l'organisation et ses attentes.

La mise en place de procédures qualité peut permettre de diminuer le risque de cyberattaques et/ou d'en limiter l'impact. Les méthodes de l'assurance qualité du développement logiciels font progresser la sécurité des logiciels tant développés en interne qu'externalisés. Bien comprendre « la gestion des normes » est obligatoire étant donné que la sécurité de l'information est « régie » par plusieurs normes (27001, 27134, ...).

expérience

Groupe Afnor : récit de la cyberattaque et rebond

Par Frédéric LECONTE, Directeur des Systèmes d'Information du Groupe Afnor.
Interview parue dans CIO Online le 10 juin 2022

Témoignage recueilli par l'AFQP Nouvelle-Aquitaine

Pouvez-vous nous relater comment vous avez découvert avoir été piraté ?

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 l'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 ?

Comment avez-vous réagi dans l'immédiat ?

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

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.

> « Alors que le sujet émergeait, nous avons rapidement communiqué. En retour, nous avons eu beaucoup de manifestations de soutien et de solidarité. »

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.

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 plateforme.

Comment avez-vous pu déployer votre communication interne ?

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.

Alors que le sujet émergeait, nous avons rapidement communiqué. En retour, nous avons eu beaucoup de manifestations de soutien et de solidarité.

Et ensuite, avez-vous pu récupérer vos données ? Comment vous y êtes-vous pris ?

Pour remonter le SI, nous nous sommes appuyés sur les experts qui nous ont accompagnés 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.

Dans l'absolu, personne n'est à l'abri d'une cyberattaque. Bien entendu, nous avons mis en place un SOC (Security Operations Center), déployé un EDR (Endpoint Detection and Response)...

Nous avons aussi mis en œuvre 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.

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.

Quelles actions et engagements menez-vous depuis ?

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.

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

©AdobeStock

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 SSPEC, 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.

ZOOM SUR
AFNOR SPEC

Par Julie LATAWIEC, Responsable Développement et Innovation secteur Numérique du Groupe Afnor

Afnor anime une commission de normalisation Cybersécurité, particulièrement active, qui rassemble un grand nombre d'acteurs français publics et privés. Ces acteurs contribuent à l'élaboration de normes sur la cybersécurité, souvent d'ampleur internationale, avec pour objectif d'aider les organisations à mieux s'organiser, à se préparer à un événement cyber.

Les normes cyber sont des outils qui permettent de renforcer la robustesse des systèmes d'information. La plus connue est la norme ISO 27001 « Systèmes de management de la sécurité de l'information ». La mettre en œuvre dans votre organisation permet de s'assurer que tous les processus sont en place pour gérer les risques et préparer les plans d'actions lors d'attaques.

Au niveau européen, le Cybersecurity Act de 2019 devrait aussi être transcrit en normes prochainement.

L'adoption de ces normes nécessite évidemment un investissement pour les organisations, bien que celui-ci reste minime par rapport aux conséquences potentielles d'un incident majeur de cybersécurité. Cependant, nous avons conscience que cela peut représenter un travail conséquent d'assimiler ces normes, surtout pour des équipes DSI et RSSI, qui ont besoin de solutions clés en main, et surtout opérationnelles.

Nous travaillons donc actuellement sur l'élaboration d'un guide AFNOR SPEC sur la continuité d'activité et la résilience des organismes suite à une cyberattaque.

Ce guide, qui sera un document de référence national et qui se veut opérationnel et facile et rapide à prendre en main, vise à recommander des bonnes pratiques à mettre en œuvre pour anticiper et se préparer à une cyberattaque, limiter son impact et assurer la continuité de l'activité de l'organisme dans le cas d'une indisponibilité prolongée du SI.

Objectifs du guide AFNOR SPEC sur la continuité d'activité et la résilience des organismes suite à une cyberattaque :
- Fournir un état de l'art des bonnes pratiques dans la perspective d'un redémarrage d'un SI dégradé par une cyberattaque.
- Envisager la continuité d'activité de l'organisation hors SI nominal en parallèle de la reconstruction du SI.
- Préparer le fonctionnement en modes perturbés/ degradés pendant une période longue (plusieurs semaines).

Ce guide AFNOR SPEC est co-élaboré par plus d'une trentaine organisations publiques et privées :
- des organisations qui ont été touchées par une cyberattaque et souhaitent faire un retex (PME, banques, grandes entreprises, hôpitaux).
- des organisations qui accompagnent les entreprises touchées par une cyberattaque (ANSSI, Orange Cyberdéfense, Ministères).
- ou tout simplement des organisations qui souhaitent échanger et partager leurs bonnes pratiques pour être prêtes lorsqu'une attaque arrive.

Le guide AFNOR SPEC sera publié en octobre 2022 et mis à disposition en téléchargement libre sur le site afnor.org.

©Fondation de la Mer

Grand Témoin


©Fondation de la Mer

Sabine ROUX DE BÉZIEUX

Présidente de la Fondation de la Mer

Afin de capitaliser des points de vue complémentaires sinon out of the box et d'ouvrir le champ des possibles, France Qualité a décidé de recueillir les réactions, avis, visions de « Grands Témoins » autour de la thématique Qualité.

Ces Grands Témoins peuvent être des dirigeants, des spécialistes connus-reconnus de tout ou partie du périmètre des démarches de progrès/de maîtrise des risques, mais également des personnalités du monde artistique, sportif, médiatique...

Découvrez la douzième interview, menée par Marie Cornet-Ashby.

Sabine ROUX DE BÉZIEUX est Présidente de la Fondation de la Mer. A ce titre, elle prend régulièrement la parole sur les enjeux concernant les océans : climat et biodiversité, lutte contre les pollutions, éducation et recherche, économie bleue et innovation, géostratégie maritime.

Elle est ancienne auditrice de l'IHEDN Enjeux Maritimes, membre du Conseil d'orientation de l'Institut de l'Océan, du Conseil supérieur de la météorologie et Capitaine de frégate dans la réserve citoyenne de la Marine nationale.

Elle est engagée depuis plus de quinze ans dans le monde des fondations, d'abord avec la Fondation ARAOK qu'elle a créée en 2005, puis au sein d'Un Esprit de Famille, qui rassemble les fondations familiales en France. Elle est par ailleurs active dans le milieu associatif, avec United Way-Alliance pour l'éducation ou Espoir Niger.

Sabine est diplômée de l'ESSEC. Après deux années en banque d'affaires, elle passe 13 ans dans le groupe Arthur Andersen à Londres et à Paris. Elle a dirigé sa structure de conseil, Advanceo, avant de rejoindre le Conseil d'administration de plusieurs sociétés cotées et de prendre la direction générale de Notus technologies, un groupe familial de PME françaises.

Sabine est également vice-présidente de la commission des affaires européennes et internationales du CESE (Conseil économique, social et environnemental) et chevalier de la Légion d'Honneur.

Sur un plan personnel, Sabine a quatre enfants. Elle a un goût prononcé pour les grands espaces et les sports d'outdoor : voile, ski et randonnée. Elle est marathonienne et triathlète.

Voir le portrait de Sabine par Les Échos : https://www.lesechos.fr/industrie-services/energie-environnement/sabine-roux-de-bezieux-entre-terres-et-mers-1369303.

QUE SIGNIFIE POUR VOUS LA QUALITÉ ?

Selon moi, le terme qualité se rapproche de la notion de perfection. En quelque sorte, une quête permanente de la qualité dans la vie, et à la fois professionnelle et personnelle. J'associerais aussi à la qualité, la sobriété et la durabilité… des valeurs transmises par mon univers familial.

Je suis Présidente de la Fondation de la Mer, et j'ai cette conscience de l'enjeu que représente la soutenabilité de la croissance pour la survie de la planète. Il nous faut imaginer des produits consommables par sept milliards de personnes, tout en préservant les ressources de cette planète. Cela induit une transformation de nos modes de production et de consommation. C'est à la fois un enjeu de qualité de vie, mais aussi une opportunité de marché incroyable !

> « Le terme qualité se rapproche de la notion de perfection. »

Finalement, le plus bel exemple de qualité est la nature elle-même, et dans sa sobriété. Elle est le socle des actions de la Fondation de la Mer.

COMMENT EN PARLER PLUS ET MIEUX ?

Je dirais par l'éducation, et en parler plus en collaborant étroitement avec les écoles. La Fondation de la Mer a signé une convention avec le ministère de l'Éducation nationale, de la Jeunesse et des Sports. Et nous proposons avec la Direction générale de l'enseignement scolaire, des outils pédagogiques afin de sensibiliser et de former tous les élèves, à l'ensemble des enjeux liés à l'Océan. Au-delà du constat établi, nous leur expliquons l'importance d'agir à tous les niveaux pour préserver notre environnement vital. À titre d'exemples pour les enfants, en consommant des produits bruts et en utilisant les poubelles pour les déchets. Pour les plus grands, la sensibilisation portera sur la meilleure façon de choisir ses loisirs, ses vêtements, son alimentation.

Grâce aux réseaux de l'Éducation nationale, nous visons les 12 millions d'élèves en âge scolaire. En parler mieux aussi, grâce à la rigueur scientifique des propos tenus, un engagement de la Fondation de la Mer.

QU'EN EST-IL DE VOTRE PARCOURS PERSONNEL ET DE VOS CENTRES D'INTÉRÊT À CET ÉGARD ?

La mer représente 71 % de la surface de la planète et la France a le plus vaste espace maritime au monde. L'Océan est ma passion ; ma conviction est qu'il est crucial de le préserver afin d'assurer notre avenir. Les leviers d'actions sont nombreux : les enfants, la science, les associations, les entreprises, les États.

La Fondation de la Mer construit pour tous des projets de qualité, scientifiquement validés, et permettant de transformer l'ensemble de ces populations en acteur positif vis-à-vis de l'Océan.

QUELLE EST POUR VOUS LA SYMBOLIQUE DU MOT QUALITÉ ?

L'être humain est une partie intégrante de la nature. C'est aussi l'espèce qui a le plus transformé cette nature pour son propre développement. Le progrès humain induit une responsabilité immense, celle de ne pas dégrader la nature à laquelle nous appartenons. Nous nous devons de trouver des modèles permettant la soutenabilité et la durabilité. Il nous faut protéger la biodiversité, c'est-à-dire la diversité de vie, sur notre planète.

La qualité, c'est le respect de la nature dans tout ce qu'elle a de beau, de divers, de multiple, d'ingénieux !

LA QUALITÉ AU SERVICE DE VOTRE ACTION, SOUS QUELLES FORMES ?

La Fondation de la Mer place la science garante de la qualité, dans toutes ses actions.

La dégradation de la qualité de l'air, de l'eau et des sols a un effet immédiat sur la santé humaine ; les impacts de l'exposome sont réels. Nous travaillons avec des scientifiques, des associations de terrain, des entreprises, des enseignants afin d'apporter des solutions à l'altération de notre qualité de vie. À titre d'exemple, notre programme SOS Corail propose des projets en crowdfunding de protection et de restauration des coraux, des mangroves, des herbiers.

La qualité de l'eau est aussi une composante de la qualité de vie. La Fondation de la Mer accompagne les entreprises dans la soutenabilité et la durabilité de leurs modèles en relation avec l'Océan. Notre outil « Ocean Approved » leur permet de mesurer leur impact sur l'Océan, et de concevoir des plans d'action pour le réduire. À travers l'obtention de ce label, l'Océan approuve la manière dont l'entreprise s'organise pour sa bonne santé.

La pollution reste omniprésente avec la présence de déchets comme... le plastique sur le littoral : 250 associations collaborent avec la Fondation de la Mer dans des collectes de déchets. Pas moins de 35 000 bénévoles ont participé à « Un Geste Pour la Mer ».

La qualité de notre action, c'est donc l'impact, que nous mesurons en permanence, pour le bien de l'Océan.

QUELS SONT LES PILIERS DE LA QUALITÉ AU SEIN DE VOTRE STRUCTURE OU DE VOTRE ACTIVITÉ ?

Je parlerais de rigueur et de qualité des projets proposés par la Fondation de la Mer à nos partenaires, et de qualité des organisations avec qui nous travaillons.

Nous octroyons des bourses à des jeunes doctorants sélectionnés pour la qualité de leurs travaux. Notre Conseil scientifique de très haut niveau est composé en partie d'Inspecteurs généraux de l'Éducation nationale. Il sélectionne les projets proposés par la Fondation de la Mer, et il valide aussi les outils pédagogiques à destination des enfants. Le label « Ocean Approved » pour un océan durable a été conçu avec le BCG, et le Bureau Veritas en lien avec le ministère de la Mer.

La qualité « irrigue » la Fondation de la Mer... le gage de respect dû à l'Océan qui a vu naître la vie sur terre.

UN OBJET VOUS INSPIRE QUAND IL EST QUESTION DE QUALITÉ ?

Un beau spi pour sa finesse, sa technicité, sa puissance incroyable. Je citerais aussi les foils des bateaux de course.

UNE PERSONNALITÉ QUI REPRÉSENTE POUR VOUS LA QUALITÉ ?

Je dirais Monsieur de La Pérouse, un grand navigateur. Charles Darwin, il s'est laissé enseigner par la nature avec humilité. Deux immenses « aventuriers » curieux de science !

UN LIEU LORSQU'IL S'AGIT DE QUALITÉ ?

La nature en général, et la mer en particulier !

LA QUALITÉ, POUR QUELLES RAISONS ESSENTIELLES ?

Sans qualité, il n'y a ni soutenabilité et ni durabilité : c'est la bataille à accélérer aujourd'hui, que l'on soit un citoyen, un consommateur ou une entreprise.

ZOOM SUR

LA FONDATION DE LA MER

Face à l'urgence climatique et à la dégradation de la vie dans l'Océan, des personnalités engagées du monde maritime et de la société civile ont créé en juin 2015 la Fondation de la Mer pour répondre aux différents enjeux liés à l'Océan.

La Fondation de la Mer est au service de tous ceux qui agissent pour un Océan durablement protégé, exploité avec soin et sagesse. Elle soutient des centaines d'acteurs locaux pour renforcer et accélérer leur impact positif en faveur de l'Océan. Elle met également en œuvre ses propres programmes pour protéger la biodiversité marine, lutter contre les pollutions en mer, soutenir la recherche, encourager l'innovation, informer et sensibiliser tous les publics.

Sabine ROUX DE BÉZIEUX, sa Présidente, est animée d'une ambition unique : réconcilier économie et écologie, science et investissement, spécialistes et citoyens. Afin d'intégrer l'Océan au cœur de la gestion des entreprises, la Fondation de la Mer a lancé en juin 2021 le label Ocean Approved, premier label mondial permettant de distinguer les entreprises qui s'engagent à prendre en compte et améliorer leur impact sur l'Océan. Accessible aux organisations de tous pays, quels que soient leur secteur d'activité et leur taille, il valorise les entreprises qui s'engagent dans une démarche d'amélioration continue de leurs impacts sur l'Océan.

Site web : www.fondationdelamer.org

FONDATION DE LA MER

#EtudierEnAveyron : qualité, sécurité, environnement au sein de Campus XIIe Avenue

Par Michaël ALBO, Responsable pédagogique Campus XIIe Avenue

Entreprise adhérente de l'AFQP Occitanie

La filière QSE du Campus XIIe Avenue s'inscrit dans un environnement composite tant au niveau des formations que des partenaires. Notre mantra, « à la rencontre de talents », est là pour rappeler que Campus XIIe Avenue est au service des entreprises pour leur apporter les compétences répondant à leur besoin dans les domaines de l'informatique, du tourisme, de la gestion et du commerce et donc du QSE.

©Campus XXIIe Avenue

La filière QSE est composée de deux formations, une Licence Professionnelle en Qualité, en partenariat avec l'IUT de Rodez et un titre professionnel Bac +5, Manager des risques QSE, en partenariat avec le réseau des IEQT. L'offre de formation vient compléter le BUT QLIO (Qualité/Logistique) dispensé par l'IUT, faisant de Rodez la seule ville d'Occitanie avec une filière complétement intégrée allant du Bac au Bac +5 sur les thématiques QSE. La filière accueille 70 étudiants par an qui sont tous en alternance. Outre les partenaires dans le domaine de la formation, Campus XIIe Avenue collabore avec l'Afnor mais aussi France Qualité, en étant acteur des actions, des projets et des études auxquels nous nous associons.

La Licence professionnelle Animateur Qualité est la formation historique puisqu'elle a ouvert en 1995, avant même la création des Licences Pro. Elle a évolué et continue d'évoluer en même temps que le métier, les normes, l'environnement, les parties prenantes mais aussi en intégrant dans son programme les dernières tendances comme la digitalisation ou la RSE. Cette évolution s'est appuyée sur la démarche qualité interne permettant de faire tourner la boucle de l'amélioration continue et ainsi répondre au mieux aux attentes des étudiants, des entreprises et de nos partenaires. La qualité est aussi développée dans le programme du Bac +5 dans une logique de management intégré QSE.

Les deux formations développent également les sujets connexes mais faisant aujourd'hui partie intégrante du bagage des manager QSE. Le Lean, la cybersécurité ou la RSE font ainsi l'objet d'actions pédagogiques particulières. Le réseau des IEQT a développé pour le Manager des Risques des parcours spécifiques sur le Lean ou la cybersécurité, permettant aux apprentis de valider des qualifications par des certifications Green Belt ou ANSSI. La RSE est, elle, principalement abordée par des actions de terrain, en lien avec des associations ou des entreprises. Les apprenants organisent des collectes ou des sensibilisations permettant de développer leur engagement citoyen en même temps que leur compétence en management de projet. Sur le Licence Pro, le projet RSE fait partie intégrante du système d'évaluation. Les apprenants ont par exemple organisé des collectes en faveur de la pratique sportive, des personnes en situation de handicap, de l'environnement ou sensibilisé aux circuits courts, au gaspillage alimentaire ou à la réparation des objets.

Les deux formations ont depuis toujours essayé de se rapprocher du monde professionnel. À ce titre, des visites sont organisées, avec les enseignants, favorisant la compréhension des apports théoriques par la découverte de bonnes pratiques au sein


©Campus XXIIe Avenue


©Campus XXIIe Avenue

des entreprises locales. C'est toujours avec cette philosophie que l'apprentissage de la pratique de l'audit ou du diagnostic réglementaire est déployé. Par groupes, et encadrés par des professionnels, les candidats préparent ces missions puis se rendent dans les entreprises pour leur apporter leur expertise, en même temps qu'ils éprouvent leur bonne appropriation des outils. Ces missions se concluent par la remise de leur rapport qui permet aux entreprises de corriger et d'améliorer leurs pratiques.

Un tel lien avec le monde professionnel est renforcé par la présence majoritaire de professionnels dans l'équipe pédagogique. Des consultants mais aussi des salariés dispensent leur expertise en l'agrémentant de leur pratique quotidienne du métier. Ces apports permettent de sensibiliser les futurs diplômés aux difficultés inhérentes au métier, en particulier, l'appropriation des pratiques et des outils par les équipes. Avec l'expérience acquise via la mission qu'ils déploient dans leur entreprise d'accueil, le contact et le vécu des enseignants accélèrent leur apprentissage de la fonction et pas seulement des outils.

Cette volonté se traduit également par l'intégration de nombreux diplômés des deux formations dans l'équipe pédagogique. Outre l'enseignement, les anciens accompagnent les candidats lors des audits ou prodiguent leurs conseils dans les différents jurys qui jalonnent les formations. Leur apport ne se mesure pas seulement à leur compétence - ils connaissent l'école et sont les garants des valeurs de travail, de transmission, de bienveillance, et d'accompagnement des nouvelles générations. Ils sont également des vecteurs importants pour appuyer le message d'exigence qui est celui des enseignants mais surtout des entreprises. Ils sont enfin un exemple dont peuvent s'inspirer les étudiants quant à leur parcours et à leurs réussites. C'est en particulier le cas des candidats lauréats et nominés au prix étudiant France Qualité. La valorisation de cette expérience permet de challenger les promotions en cours pour être sélectionné et représenter l'établissement à l'édition suivante.

Ces nombreux échanges avec les professionnels de la qualité, les maitres d'apprentissage au cours des visites pédagogiques et la participation aux différents ateliers ou forums organisés par France Qualité, permettent de faire évoluer les contenus pédagogiques. Il y a le sentiment que la qualité évolue mais doit encore évoluer pour s'intégrer plus naturellement dans les organisations. On retrouve encore une dichotomie entre la qualité du produit et le management. La production voit en la qualité un outil de traçabilité et d'amélioration visant à sécuriser l'entreprise au regard du risque client et améliorer la performance industrielle. Le management voit en la qualité une opportunité de rationaliser le pilotage de l'organisation et de s'appuyer sur ses principes et ses outils pour déployer des démarches RSE ambitieuses. Tous sont à la recherche d'un équilibre dans des systèmes qui sont de plus en plus lourds, complexes et difficiles à faire vivre. La digitalisation est une formidable opportunité qui doit permettre de simplifier les flux et faciliter les interactions entre les différentes activités. Elle doit permettre de concentrer les ressources sur la création de valeur par l'intelligence collective au service des clients, avec l'objectif d'améliorer les performances économiques et industrielles tout en jouant son rôle social et sociétal que ce soit auprès des collaborateurs, de l'environnement.

C'est cette vision qui est partagée avec les apprentis et qui a conduit à la prise en compte du Lean, de la cybersécurité ou de la RSE. C'est toujours cette vision qui fait évoluer la pédagogie et l'organisation en digitalisant les process pour plus de flexibilité, de réactivité et de simplicité.

CAMPUS XII AVENUE
à la rencontre de talents

www.campus12avenue.fr

FRANCE QUALITÉ

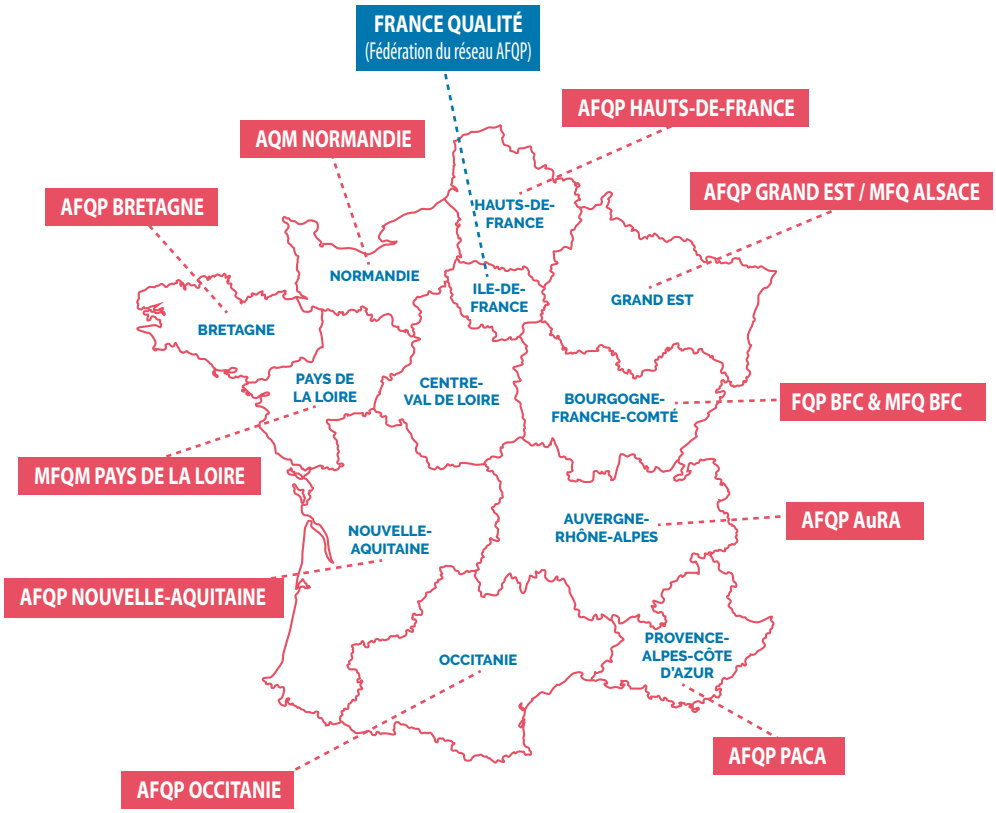
EXCLUSIVITÉ ADHÉRENTS

Revue Echanges
Livres Blancs
Replays
...

A compter de 2022, seuls les adhérents du réseau France Qualité ont accès à l'intégralité des productions de l'association.

J'en profite

REJOIGNEZ LE RÉSEAU FRANCE QUALITÉ



RETROUVEZ LES COORDONNÉES DES ASSOCIATIONS RÉGIONALES SUR :

www.qualiteperformance.org/rejoindre-lafqp