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

5 LE DOSSIER
CYBERSÉCURITÉ ET QUALITÉ

CONTEXTE
6- CYBERSÉCURITÉ, DE QUOI PARLE-T-ON ?

ANALYSE
12- CYBERSÉCURITÉ ET QUALITÉ : UNE ALLIANCE DE CŒUR ET DE RAISON

TENDANCE
15- L'EMPLOI CYBERSÉCURITÉ EN HAUSSE

TÉMOIGNAGE
16- LA CYBERSÉCURITÉ VUE PAR INKIVARI

EXPÉRIENCE
18- GROUPE AFNOR : RÉCIT DE LA CYBERATTAQUE ET REBOND

21 GRAND TÉMOIN
SABINE ROUX DE BÉZIEUX, PRÉSIDENTE DE LA FONDATION DE LA MER

24 ENSEIGNEMENT
CAMPUS XIIE AVENUE

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.

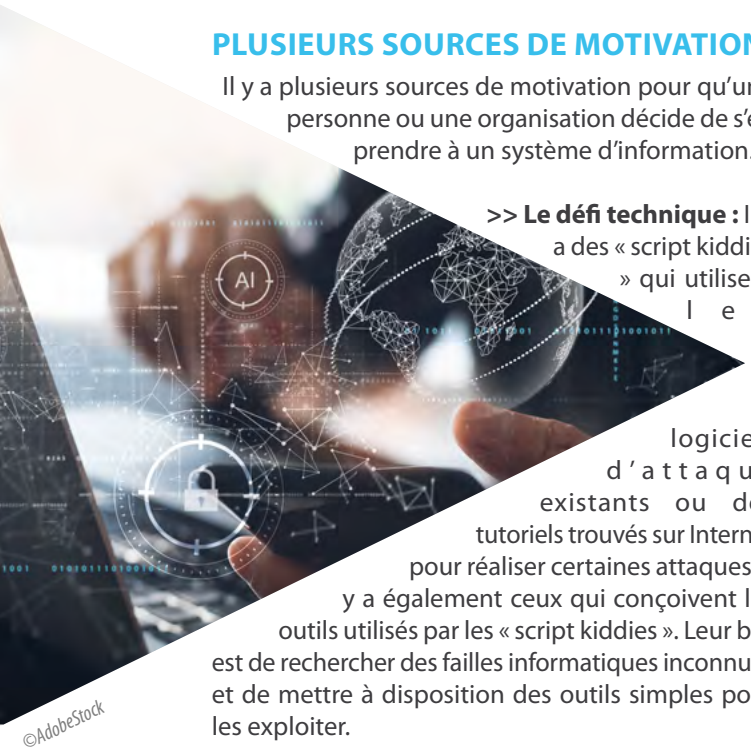
>> Les adwares

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

LA SUITE DE CE CONTENU EST RÉSERVÉE AUX ADHÉRENTS DU RÉSEAU FRANCE QUALITÉ

WWW.QUALITEPERFORMANCE.ORG

FRANCE QUALITÉ

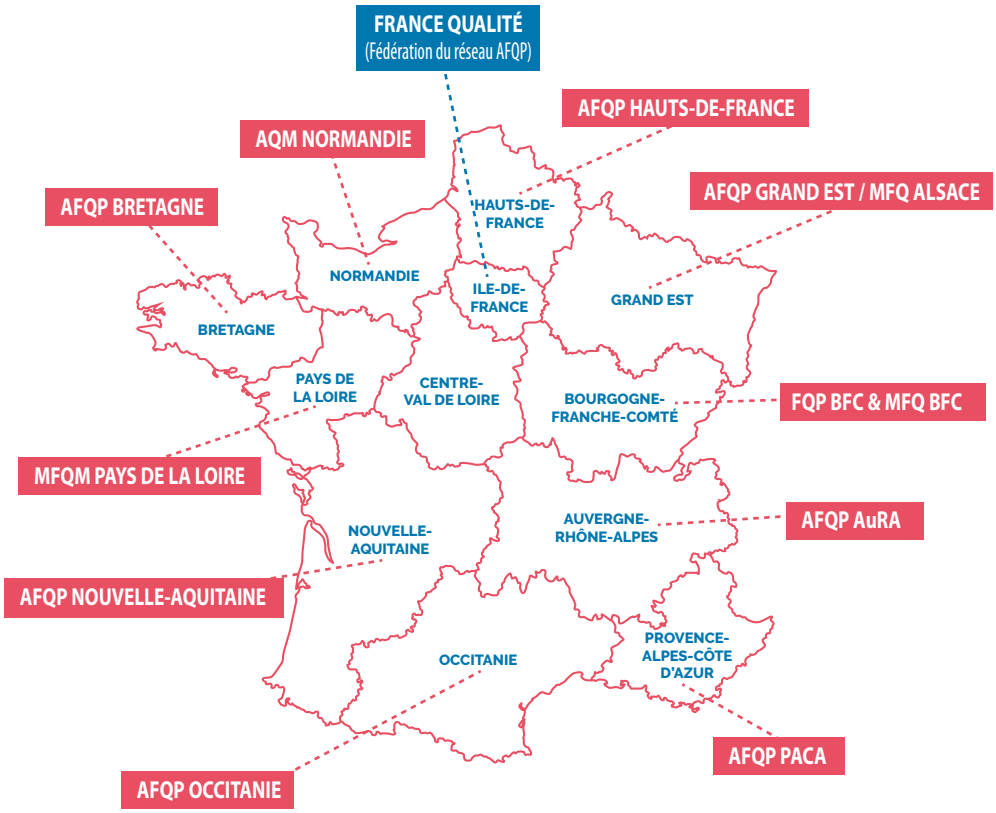
EXCLUSIVITÉ ADHÉRENTS

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