LIVREBLANC

GUIDE POUR UN **BON USAGE** DES **OUTILS NUMÉRIQUES**

DANS UN CONTEXTE DE CYBERMALVEILLANCE ET DE RENFORCEMENT DE LA LÉGISLATION

by FRP2i
La Fédération des Revendeurs et Prestataires Informatiques Indépendants

Sommaire

1 p4 LA SÉCURISATION **PHYSIQUE DES LIEUX** DE STOCKAGE DE DONNÉES

2 p6 LA SÉCURISATION DES **ACCÈS** AU RÉSEAU **INTERNE**

3 p8 LA **SAUVEGARDE** DES DONNÉES

4 p10 LE CHOIX DES **MOTS DE PASSE**

5 p12 LES **COURRIELS**

6 p14 **INTERNET**

7 p16 LA SÉCURITÉ DU **POSTE INFORMATIQUE**

8 p18 L'UTILISATION DES **OBJETS CONNECTÉS PERSONNELS** EN ENTREPRISE

9 p20 LA SÉCURISATION DU **RÉSEAU EXTERNE** DE L'ENTREPRISE

10 p22 NE PAS LAISSER DE **TRACE**

11 p24 BIEN CHOISIR **SES PARTENAIRES**

12 p26 DIRECTIVE **RGPD**

13 p28 EN CAS DE **DOUTE**

14 p30 SE POSER LES **BONNES QUESTIONS**

Ils ont contribué à la rédaction de ce guide :

Dominique NORMANDIN
Spécialiste en sécurité
et réseau informatiques
Intervenant à l'IUT de Clermont Ferrand et en centres de formation

« La sécurité doit toujours être considérée et abordée de façon globale : il faut engager une réflexion générale sur le système d'information avant d'envisager une stratégie de sécurisation. En cela, la mise en conformité des structures vis-à-vis de la loi européenne RGPD peut et doit permettre aux organisations de comprendre et de mieux sécuriser les flux des données à caractère personnel. »

« La sensibilisation et la formation autour des sujets de cyber-sécurité doivent être des impératifs chez les éditeurs de solutions de sécurité. Cela se traduit par des opérations de communication d'envergure, et l'accompagnement des partenaires. L'objectif est de répondre aux exigences de sécurité minimale et aux nouvelles obligations imposées par le RGPD. A l'ère du « tout numérique », préserver la confidentialité des informations à caractère personnel ou stratégiques face à des menaces toujours plus sophistiquées et des attaquants déterminés est l'affaire de tous. »

Benoit GRUNEMWALD
Cybersecurity Leader
Eset France et Afrique Francophone

Jean-Sébastien MARIEZ
Avocat spécialiste droit numérique
Barreau de Paris – Cabinet DE GAULLE FLEURANCE & Associés.

« La sécurité des données personnelles est un élément central du plan de conformité que toute entreprise doit mettre en place afin d'anticiper l'application à compter du 25 mai 2018 du Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD). »

« La multiplication et la diversification des usages sur les réseaux obligent à la plus grande prudence et au plus grand soin dans la mise en œuvre des processus de sécurisation. Le réseau local doit participer activement à la politique de sécurité de l'entreprise afin de garantir l'intégrité des données et le bon fonctionnement du réseau pour chaque utilisateur, chaque usage. »

Thierry DOUALAN
Product Manager
chez D-Link France

Emmanuel ANDRÉ
Président de la Fédération des
Revendeurs et Prestataires
Informatiques Indépendants

« La sécurité informatique est un défi quotidien : prévention des dysfonctionnements matériels, des pannes logicielles, prévention des actes de cybercriminalité, prévention des erreurs humaines. Les collectivités, PME, TPE sont encore peu ou pas sensibilisées à ces phénomènes. Les conséquences sont pourtant terribles pour les organisations non préparées. »

1

LA SÉCURISATION **PHYSIQUE DES LIEUX** DE STOCKAGE DE DONNÉES

Sécuriser un système informatique ne sert à rien si ce dernier est facilement accessible ! Le vol physique de postes de travail, ou pire de serveurs, permet, une fois le matériel récupéré, de prendre tout son temps pour analyser et passer outre les sécurités mises en place.

CE QU'IL FAUT RETENIR

- L'accès physique à l'organisation et donc aux postes et systèmes informatiques doit être sécurisé.
- Les lieux doivent être difficilement accessibles, même quand l'établissement est ouvert.
- Les systèmes de vidéo surveillance ou déclenchement de brouillard n'empêchent pas les infractions, mais peuvent les retarder.
- Les visiteurs doivent être accompagnés.

C'est la première règle :

faire en sorte que les systèmes informatiques ne puissent pas être dérobés.
Les lieux doivent donc être protégés, difficiles d'accès une fois l'établissement fermé au public. La mise en place de systèmes de fermetures avec des serrures difficilement fracturables, la sécurisation des locaux par systèmes d'alarme, des systèmes de reconnaissance de droit d'accès, de détection de présence, détection d'ouverture sont nécessaires.
Cet aspect est souvent négligé, mais il est important, car il retarde le vol : écrans, PC et portables devraient être reliés à des kits antivols, solidement fixés au sol ou à un mur.

Selon les infrastructures,

il devrait exister : sas d'entrée, registre des entrées/sorties de visiteurs et l'accompagnement systématique et constant des visiteurs dans les locaux. Les accès secondaires (quais de chargement, lieux d'enlèvement, entrées annexes) doivent répondre aux mêmes règles.

Pour le personnel itinérant

disposant de tablettes, ordinateurs portables et smartphones, il est important d'interdire la visibilité de ces appareils mobiles dans les véhicules, chambre d'hôtels… en ne laissant pas ces appareils disponibles à la vue, pour réduire les risques de vols : une voiture n'est pas un coffre-fort.

Dans les locaux,

en cas d'accès indésirables, les systèmes de déclenchement de brouillard s'avèrent très efficaces. Les systèmes de vidéo surveillance avec alerte en temps réel sur smartphone sont également des solutions permettant d'être averti « en direct » d'une intrusion en cours dans le pire des cas, d'une intrusion allant se produire dans le meilleur des cas.

Pour les serveurs de données

ou d'applications ainsi que pour les serveurs NAS faisant office de stockage ou de sauvegarde centralisée, il est nécessaire de sur-sécuriser le local hébergeant ces systèmes, afin de retarder ou d'empêcher l'accès physique à ces éléments critiques.

2

LA SÉCURISATION DES **ACCÈS** AU RÉSEAU **INTERNE**

Laisser un tiers (représentant, client, fournisseur, personne extérieure à l'établissement…) se connecter à votre réseau internet est devenu une pratique courante. En se connectant ainsi à internet, il se connecte aussi à votre réseau informatique.

CE QU'IL FAUT RETENIR

- A chaque fois que cela est possible : privilégier un réseau informatique filaire plutôt que wifi.
- Interdire à un « invité » toute connexion si le réseau de l'organisation ne gère pas de réseau public.
- Un matériel professionnel conforte la sécurité de base d'un réseau.
- La mise en place est complexe : elle doit être réalisée par un spécialiste.

Dans la mesure du possible, il est

CONSEILLÉ D'INTERDIRE toute connexion à votre réseau par des tiers qui ne font pas partie de votre organisation.

Cependant, pour les organismes souhaitant offrir cette possibilité, il est nécessaire de scinder le réseau interne de l'organisation d'une part et l'accès externe d'autre part, afin de pouvoir continuer à offrir cette facilité de connexion à internet, tout en bloquant l'accès à vos postes informatiques. Pas nécessairement parce que le tiers qui s'y connecte aurait de mauvaises intentions. Ce n'est peut-être pas le cas. Mais parce qu'à son insu, son appareil numérique (portable, tablette, ou smartphone) peut être porteur d'éléments malsains qui peuvent contaminer vos propres postes. Bloquer l'accès à votre réseau interne est donc une sécurité nécessaire.

Et ce tant pour les connexions wifi que pour les connections filaires. Il est nécessaire de s'équiper de commutateurs réseaux, dits « Switchs », qui soient administrables, permettant ainsi de segmenter le réseau local en plusieurs sous réseaux (réseaux virtuels, dits « Vlans ») plus sécurisés.

Avec de telles solutions matérielles, il est ainsi possible de dissocier les réseaux : en créant un réseau « invité », où seul internet sera accessible depuis un point identifié, tandis que sur votre réseau « privé », l'ensemble de vos postes communiquent entre eux sans être ni vus ni accessibles par le réseau « invité ».

Dans la mesure du possible, il est

DÉCONSEILLÉ D'ACTIVER un réseau Wifi en entreprise.

Les données qui transitent en Wifi sont facilement récupérables et exploitables par un utilisateur averti ou mal intentionné. La connexion par câble Ethernet, dite connexion filaire, est un choix qu'il faut privilégier à chaque fois que cela est possible. La connexion filaire bénéficie de 2 avantages : sa sécurité renforcée par rapport au wifi et sa vitesse de connexion.

Si la mise en place d'un réseau Wifi est incontournable :

Dans certains cas (utilisation de portables, de tablettes), l'utilisation du Wifi est une obligation. Alors il est nécessaire de sécuriser l'accès par la création de Vlans (réseaux virtuels), par une gestion très stricte des équipements connectés et par une politique de sécurité respectant des règles qui doivent être régulièrement remises en causes. Seuls les équipements informatiques de l'entreprise doivent pouvoir se connecter sur le réseau privé. Les équipements actuels professionnels permettent de reconnaitre ces appareils et de n'autoriser que ceux-ci sur le réseau.

Les cybercriminels ont trouvé la parade à cette sécurité, avec la technique du « Mac Spoofing » (se faire passer pour un équipement reconnu et autorisé sur le réseau), mais la mise en œuvre est complexe et ne reste accessible qu'à certains.

Afin de limiter les risques

- **Il est tout de même nécessaire de configurer le réseau Wifi avec un système de chiffrement** : TKIP (WPA) ou AES (WPA2) et d'authentification forte : WPA-SPK (clé partagée) ou WPA-EAP (certificat).
- **Il est également important de s'assurer qu'aucun équipement ne puisse se connecter à un réseau Wifi de type P2P** (peer-to-peer ou pair à pair en français), ni qu'il puisse accéder en même temps au LAN et au Wifi, ceci afin d'éviter les attaques de type pontage (anti-hybrid network bridging).
- **Le point d'accès Wifi doit être en mesure d'enregistrer un journal de connexions**, qui doit être régulièrement vérifié. Il doit également être en mesure de gérer des plages horaires de connexions, permettant ainsi de stopper tout accès Wifi en dehors des jours et heures d'ouverture de l'établissement. La mise en place d'un contrôleur Wifi facilite la maintenance et la gestion des points d'accès, sécurise l'ensemble du réseau (possibilité de mise en quarantaine).
- Enfin, si pour des raisons de convenances, vous disposez d'un Wifi « Public » pour autoriser vos visiteurs à se connecter à internet, **la clé d'accès wifi publique doit être changée chaque jour.** En référence : loi n° 2006-604 du 23 janvier 2006.

DANS TOUS LES CAS

la sécurité d'un réseau informatique est une tâche complexe, qui doit être confiée à un professionnel ayant de solides compétences et expériences dans ce domaine. La mise en place et la gestion des réseaux virtuels, de l'authentification, de VPN, de contrôle de flux est un métier de spécialiste.

3

LA SAUVEGARDE DES DONNÉES

Dans le domaine de l'informatique, Il y a 2 types de clients : ceux qui ont déjà perdu leurs données, et ceux qui vont les perdre.

CE QU iL FAUT RETENiR

- Aucune organisation n'a été, n'est, ne sera épargnée par la perte de données. Trop peu y sont préparées.
- Les supports externes de type USB sont à bannir.
- La multiplication des sites de stockage des sauvegardes (interne + externe) est un gage de sécurité.
- Une stratégie de sauvegarde se planifie, s'organise, se contrôle, se vérifie.
- Techniquement, l'infrastructure réseau doit être optimisée pour que les process de sauvegardes ne créent pas de ralentissements sur les postes de travail.

Des chiffres :

Il y a **80 %** de chances pour que la prochaine atteinte à l'intégrité du système/des données provienne de l'intérieur même de votre organisation.
50 % des entreprises qui subissent un désastre numérique disparaissent dans les 4 années qui suivent.
Lorsque la sauvegarde des données est lancée manuellement par un utilisateur, elle est en moyenne lancée **1 fois sur 17** seulement.
En France, le coût annuel généré par les interruptions de service informatique et les pertes de données est estimé à de plus de **40 milliards** d'**Euros**.

Il existe de nombreux moyens d'assurer la sauvegarde des données. Tous ne sont pas fiables. Dans le cadre d'un usage professionnel, les « clés Usb » et « disques externes » doivent être bannis ! Ce sont des solutions dédiées à un usage privé, pour assurer la sauvegarde de 2 albums de musique et 3 photos… mais sûrement pas les données d'une entreprise car leur fiabilité, leur risque de perte, de panne, est un des plus élevés qui soit.
Les supports CD et DVD sont également à bannir pour plusieurs raisons : les temps de sauvegarde sont excessivement longs, les supports sont de faibles capacités et la fiabilité de ces supports dans le temps est médiocre.

La sauvegarde interne

Elle peut être réalisée sur un serveur NAS (matériel dédié contenant un ou plusieurs disques durs de grande capacité).

Avantages :
accessible par le réseau interne, le serveur NAS permet de réaliser une ou plusieurs sauvegardes par jour : le temps de sauvegarde est très rapide, se réalise en temps réel, sans impacter le fonctionnement des utilisateurs.

Inconvénient :
Le serveur NAS reste dans les mêmes locaux que les postes informatiques et, en cas d'incendie, de dégâts des eaux ou de vol, la perte peut être totale.

La sauvegarde externe

Plusieurs solutions peuvent être envisagées.

1/ **Pour maîtriser et conserver en interne l'intégralité des sauvegardes, un second serveur NAS peut être installé sur un site distant** et, à période définie (généralement à partir de la fin de la journée), le serveur NAS interne se réplique sur le serveur NAS distant. Cette méthode

Une règle importante à toujours avoir à l'esprit avec l'informatique est de ne pas faire confiance à l'informatique ! Ni aux machines, ni aux utilisateurs.

est couramment utilisée, mais est contraignante : elle impose un double investissement au niveau des serveurs NAS d'une part, une connexion internet de très grande qualité et très rapide d'autre part. Enfin, elle suppose que l'entreprise dispose d'au moins 2 sites, physiquement éloignés l'un de l'autre, bénéficiant chacun de connexions internet « robustes ».

2/ La sauvegarde « Dans le Cloud ».
Il est nécessaire de sélectionner un hébergeur agréé. Certains corps de métiers (santé, industries sensibles, collectivités, entreprises intervenant pour l'armée et l'industrie militaire) sont tenus à des obligations strictes. Les pseudo-hébergeurs (fournisseurs d'accès, sites internet…) ne sont pas recommandés pour le peu de garanties de sécurité proposées, par le flou concernant la localisation des centres de sauvegardes et la faiblesse ou l'absence de chiffrement et de confidentialité des données sauvegardées.
Il est donc nécessaire de se rapprocher d'un hébergeur fiable, proposant le chiffrement des données sauvegardées dès leurs transmissions depuis le poste client : la transmission doit être chiffrée de bout en bout. D'autre part, certains hébergeurs professionnels proposent désormais une rétention des données sur plusieurs semaines, mois, années, permettant ainsi plusieurs « points » de sauvegarde. En cas d'attaque par un virus de type crypto-locker (qui a pour but d'encoder les données clients pour les rendre inaccessibles), il est possible de récupérer les données issues de plusieurs sauvegardes, permettant ainsi d'avoir une véritable solution de reprise d'activité, et non pas seulement la dernière sauvegarde réalisée, pour peu que celle-ci soit déjà infectée par le virus et devienne donc inexploitable. Les hébergeurs professionnels réalisent eux-mêmes une sauvegarde de leur data-center (centre de sauvegarde) sur un second site distant. Dans ces conditions, la sécurité des données est particulièrement fiable.

Fréquence
Une sauvegarde opérationnelle est une sauvegarde quotidienne, voire multi-quotidienne !

Vérification
La vérification régulière de l'intégrité des données sauvegardées est un impératif. Cette vérification permet de certifier que la restauration des données en cas d'incident est possible.

Automatisation
Le processus de sauvegarde doit-être automatique : ce n'est ni à un utilisateur ni à un administrateur d'avoir à « lancer la sauvegarde ».

Mise en place
Il est impératif de mettre en place une véritable stratégie de sauvegarde et de la remettre en cause régulièrement.

4

LE CHOIX DES **MOTS DE PASSE**

La plupart des cas de piratage ou d'intrusion est liée à la facilité à découvrir un mot de passe trop simple, trop court, trop évident, trop « 1234 ».

CE QU'IL FAUT RETENIR

- Un mot de passe doit être complexe
- Pour les applications et sites sensibles (données confidentielles, banque), il doit être régulièrement changé.
- Ceux fournis par défaut sur le matériel des constructeurs doivent être modifiés à la première mise en route.
- Un référent informatique doit être nommé : il doit pouvoir accéder à l'ensemble des ressources des utilisateurs.

1/ Les mots de passe doivent être mémorisés et non pas inscrits.
Ils ne doivent pas être regroupés dans un fichier « Excel ». Pire, ils ne doivent en aucun cas être sauvegardés dans le « cloud ». Ils ne doivent pas transiter par mail sur votre messagerie personnelle ou sur la messagerie d'un collègue si les échanges ne sont pas chiffrés ! Le traditionnel papier jaune collé sur l'écran avec les mots de passe inscrits bien en évidence est à proscrire !

2/ La force d'un mot de passe réside dans sa longueur et dans sa complexité : 9, 12, 16 caractères. Il doit comprendre un mélange de lettres, de chiffres et de caractères spéciaux. Pour les lettres, c'est un mélange de majuscules et de minuscules. Un mot de passe sécurisé pourrait ressembler à cela : Y6!tpM4Rsm$(2 Inconvénient : il n'est pas forcément simple à retenir. Une méthode permettant de retenir un mot de passe complexe, mais facilement mémorisable est d'utiliser une phrase. Vous avez 4 chats et 2 chiens ? Alors voilà un exemple : « J'ai 4 chats : Horos, Gribouille, Toupie, Gandhi, et 2 chiens : Plouf et Zig-Zag ». Traduit en mot de passe, cela donne : J'a4c:HGTGe2c:PZ (La première lettre de chaque mot est récupérée pour générer le mot de passe).

3/ Un mot de passe basé sur un mot existant, comme un prénom, une ville, une date de naissance, un nom à l'envers, le nom d'un animal de compagnie ou celui de l'organisation est à bannir…

4/ Les mots de passe pour accéder aux sites internet sécurisés et aux applications de l'organisation doivent obligatoirement **être différents** de celui du mot de passe de messagerie.

5/ Pour les sites ou applications sensibles, il faut **régulièrement changer de mot de passe** : mensuellement ou au trimestre.

6/ Si un mot de passe est automatiquement généré par un site ou une application, il doit être **modifié dès la première connexion.**

7/ Pour les appareils permettant les connexions à internet, les commutateurs réseaux manageables, les imprimantes : le mot de passe par défaut, à la réception du matériel (admin dans 90 % des cas) doit être changé. Idem avec les appareils Bluetooth (0000).

8/ Certains navigateurs internet proposent de mémoriser les mots de passe. Cette pratique doit être évitée.

9/ L'importance du mot de passe de session sur un ordinateur est très relative, il faut moins d'une minute à une personne initiée pour le découvrir ou pour utiliser le poste sans avoir besoin du mot passe : il est donc nécessaire de chiffrer les données importantes présentes sur le poste de travail, par le biais de logiciels de chiffrement, qui sont aptes à chiffrer les fichiers que vous définirez comme confidentiels et importants et/ou l'intégralité du disque dur.

10/ Les mots de passe doivent être différents selon les applications utilisées.

11/ Le référent informatique de l'organisation ou un administrateur doit pouvoir réinitialiser les mots de passe des utilisateurs ou bien accéder à toutes les ressources via un système de secours. C'est une obligation légale de l'entreprise. Toutes ces actions doivent être tracées et enregistrées. En dehors de lui, les mots de passe ne doivent pas être divulgués : un secret connu de plus d'une personne n'est plus un secret.

12/ La sortie de veille d'un écran ou d'un poste de travail doit obligatoirement demander le mot de passe de la session utilisateur.

5 LES COURRIELS

Au rythme de 30, 50, 100 courriels par jour, le risque d'infection ou d'attaque par ce biais est un des plus importants qui soit. Il suffit d'une erreur d'appréciation et d'un clic malheureux.

CE QU iL FAUT RETENiR

- Utilisation de protocoles sécurisés pour lire / envoyer des messages.
- Personne ne vous aime !!! Soyez clairvoyant dans la lecture de vos mails.
- La messagerie doit-être adossée à un programme de sécurité.
- Les courriels confidentiels / sensibles sont envoyés de manière cryptée.

Si les courriels abolissent les délais de transmission d'informations, ils sont dans le même temps devenus encombrants, envahissants et dangereux.

Les dangers : les courriels comportant des pièces jointes infectées, les courriels mentionnant un lien vers un site internet, les courriels imitant un courriel qui pourrait être officiel et, enfin, les courriels qui proviennent d'un de vos contacts, sans que ce contact ne vous ait rien expédié !

1/ Prendre le temps de lire, de vérifier l'adéquation nom de l'expéditeur / adresse mail de l'expéditeur / contenu du mail.

2/ Ne pas ouvrir de pièce jointe si l'**expéditeur n'est pas connu.**

3/ Supprimer sans hésitation les courriels demandant des informations personnelles (mot de passe, coordonnées bancaires) ou invitant à cliquer sur un lien pour s'identifier sur un site. Il s'agit très souvent de Phishing (apparence d'une institution / entreprise), redirigeant vers un site qui « ressemble » au site officiel, mais se trouve en réalité être un « faux site », dont le but est de récupérer des identifiants de connexion.

4/ Ne pas faire suivre les courriels de type chaîne (appel à la générosité, grand malheur si non envoi du courriel à d'autre contacts, fausses alertes…).

5/ Jamais une institution n'enverra un courriel avec des **fautes d'orthographe !**

6/ Hélas non ! Vous n'avez pas gagné 20.000.000 Euros à la grande loterie organisée par Microsoft ou par un tirage au sort Européen en provenance du gouvernement Espagnol. **Les offres trop belles et irréelles, non sollicitées par vos soins, doivent être supprimées** sans regret.

7/ Si un lien est présent dans un courriel et que le courriel semble officiel, le fait de positionner la souris sur le lien indique quel site va être ouvert dans le navigateur. **Il faut s'assurer que le lien vers le site est celui qui est habituellement utilisé.** Mieux vaut opter pour le lancement de votre navigateur internet et la saisie manuelle de l'adresse du site.

8/ C'est le 1er Avril tous les jours ! **L'information annoncée dans un courriel doit être mise en doute et vérifiée.**

9/ Un programme de sécurité doit être interfacé avec le programme de messagerie : il gère le contenu des courriels d'une part et des pièces jointes d'autre part.

10/ La création de filtres pour gagner du temps : mise en place d'un dossier [SPAM] dans lequel transitent automatiquement tous les messages suspects. Ce filtre permet un gain de temps précieux en lecture.

11/ Un autre filtre avec les courriels provenant d'expéditeurs figurant dans votre carnet de contacts en créant un dossier [A LIRE]. Ce filtre permettra d'identifier plus rapidement les courriels « sûrs ».

12/ Les connexions de messagerie doivent être sécurisées : les protocoles pops, smtps, imaps sont sécurisés et doivent être préférés aux simples pop, smtp et imap.

13/ Pour les données sensibles, le courriel peut (doit) être envoyé de manière chiffrée, afin que seul le destinataire possédant la clé de déchiffrement puisse le lire.

14/ Les moyens humains et techniques à la disposition des cyber-pirates leur permettent dorénavant de cibler les entreprises de toutes tailles, les petites et moyennes n'étant pas épargnées. **N'importe quelle entreprise peut être la cible de cyber-espionnage.**

6

INTERNET

Internet est devenu incontournable : déclarations, recherches documentaires, commandes, sites internet (marchands ou vitrines), consultations… C'est aussi un fabuleux vecteur d'attaques et d'implantation de programmes espions.

CE QU iL FAUT RETENiR

- Le navigateur et les plugins doivent être systématiquement mis à jour.
- Un programme de sécurité doit surveiller la navigation.
- Les connexions « publiques » sont à proscrire sans VPN.
- Respecter une charte de bon usage d'internet.

La problématique de la navigation sur internet est complexe : les navigateurs, quels qu'ils soient (Mozilla, Google Chrome, Internet Explorer), présentent des failles de sécurité et sont régulièrement mis à jour par leurs éditeurs respectifs. Mais les navigateurs utilisent également des programmes additionnels, dits « plugins » (Java, Flash, Adobe Reader…) qui nécessitent également une attention particulière.

Au-delà de l'outil utilisé pour naviguer, **il faut également définir dans l'entreprise des règles de bonne conduite** :

1/ Ne pas laisser un navigateur internet enregistrer vos **identifiants et mots de passe**.

2/ Refuser les **changements de page d'accueil** par défaut.

3/ Refuser les **installations de barres d'outils**.

4/ Ne jamais laisser un site internet juger de **l'état des mises à jour de vos programmes.** Ce n'est pas un site internet qui doit vous avertir qu'un programme ou plugin n'est pas à jour et vous proposer, dans la foulée, de « cliquer » pour le mettre à jour. Rendez-vous plutôt sur le site de l'éditeur et téléchargez la dernière version ou bien exécutez le programme concerné et vérifiez si ce dernier propose des mises à jour.

5/ Laissez un **niveau de sécurité élevé** dans vos navigateurs : préférez avoir à « autoriser » la navigation sur les sites sur lesquels vous vous rendez couramment, en créant des exceptions.

6/ Aucune connexion sur les **bornes extérieures** avec un appareil mobile (gare, aéroport, ville, hôtel). Si cela doit impérativement être nécessaire, vérifiez que vos partages sont bloqués, n'autorisez pas le partage wifi, vérifiez les paramètres de votre firewall.

7/ La **solution de sécurité** installée sur le poste doit être **active**, à jour, et doit surveiller en permanence la navigation sur internet.

8/ Pour les postes mobiles (tablettes, portables, smartphones), aucune connexion ne doit être autorisée sur des **bornes publiques**. Des dominos, clés 3G, 4G sont plus appropriés.

9/ Aucun programme ni aucune connexion **peer to peer** ne doivent être autorisés sur un poste de travail.

10/ Une **charte de bonne conduite** doit exister dans l'organisation. Il faut se conformer à cette charte qui doit traiter des bonnes pratiques en terme de navigation internet d'une part, en terme de sécurité informatique d'autre part.

11/ Privilégier l'**utilisation de VPN** lors de connexions depuis l'extérieur de l'entreprise.

7

LA SÉCURITÉ DU **POSTE INFORMATIQUE**

C'est par le poste informatique que tout arrive. Entre erreur humaine, malveillance, dysfonctionnement matériel, les risques sont multiples et bien réels.

CE QU'IL FAUT RETENIR

- Le poste de travail est maintenu en bon état de fonctionnement.
- Il est protégé par une suite de sécurité fiable.
- Les données sensibles sont chiffrées.
- Un tiers ne connecte pas sa clé USB ou ne recharge pas son smartphone sur un poste informatique.
- Les programmes « gratuits » ne sont pas des solutions.
- Seuls vous et les personnes habilitées pouvez intervenir sur votre système informatique.

1/ La sécurité matérielle du poste est généralement assurée par la maintenance technique des équipements. C'est soit un service interne, soit un prestataire externe qui assume cette mission. Elle a pour but de maintenir un niveau de performance optimale des différents composants du poste. Les services informatiques internes, ou le prestataire, peuvent recevoir, par le biais d'utilitaires installés sur un poste de travail, son état de fonctionnement en temps réel et agir si besoin.

2/ Le poste de travail est protégé à minima par un antivirus et, idéalement, par une suite de sécurité multi-couche intégrant : Antivirus, Antispyware, Anti-phishing, Firewall et Antispam. Les mises à jour doivent être activées. La désactivation temporaire de la protection doit se faire par un administrateur, avec confirmation par mot de passe. Elle doit être motivée, tracée et enregistrée.

3/ L'insertion de support USB peut être tolérée dès lors que ceux-ci sont identifiés comme sûrs. Cependant, l'exécution automatique des programmes doit être proscrite. De plus, une analyse avec l'antivirus du support amovible est nécessaire avant d'en récupérer les données, ou d'exécuter les programmes présents sur ce support. Il est également préférable de mettre en place un système de chiffrement de ces supports externes. Le blocage total des accès USB est recommandé pour certains postes sensibles ou particulièrement exposés.

4/ La mise à jour du système d'exploitation, ainsi que des différents programmes présents sur le poste, doit être activée et il est important de vérifier que ces mises à jours sont effectives. La mise à jour des programmes permet de corriger des failles de sécurité identifiées par les éditeurs, ou apporte des améliorations de fonctionnement aux programmes.

5/ Dans la mesure du possible, **aucun périphérique étranger à l'entreprise ne doit être connecté** au poste. Sous prétexte d'avoir besoin de recharger la batterie d'un appareil mobile (smartphone), le simple fait de le connecter au poste pourrait permettre d'y implanter un programme malveillant ou de récupérer des données sensibles du poste. Des systèmes existent pour permettre le rechargement des batteries d'appareils externes, tout en bloquant les échanges entre le poste et ces appareils.

6/ Aucun **document mentionnant les mots de passe** ou données confidentielles n'est « collé » sur l'écran.

7/ N'installez aucun **programme promettant une amélioration des performances** de votre système informatique ! Les outils nécessaires au bon fonctionnement d'un poste de travail sont déjà présents sur le poste.

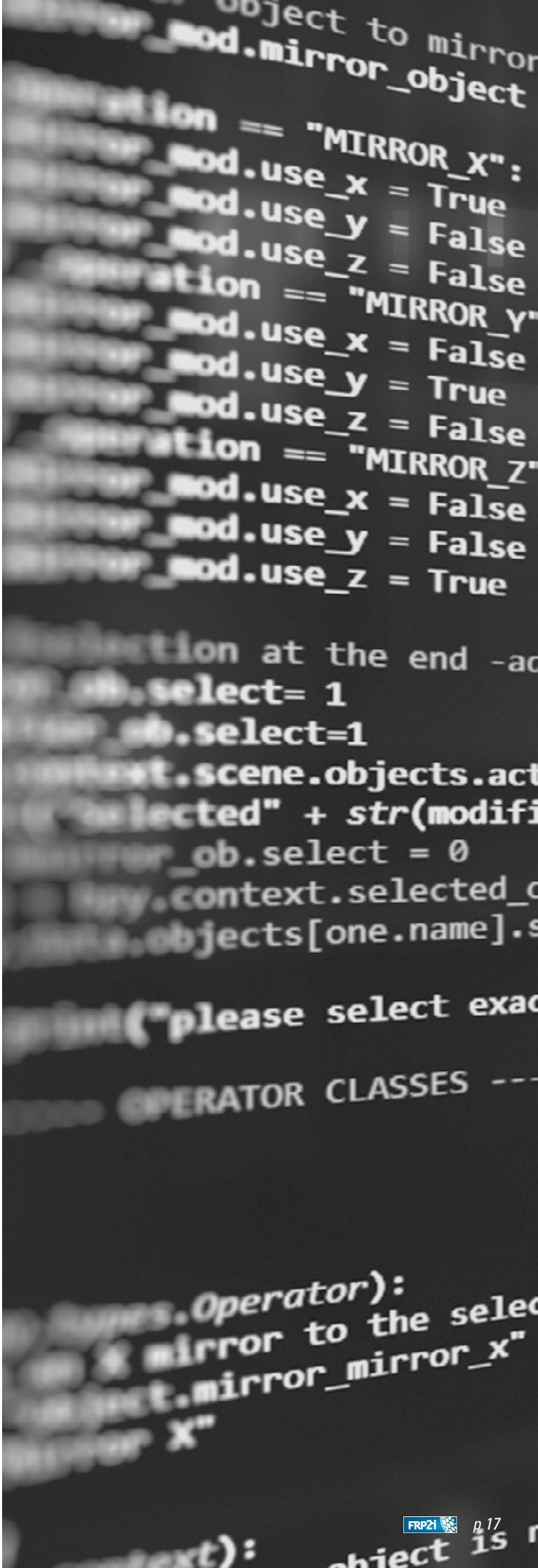
8/ Pour éviter les dégâts électriques, ou une coupure de courant pouvant provoquer un dysfonctionnement dans le meilleur des cas, une perte de données dans le pire des cas, le poste de travail sera alimenté et protégé par un onduleur, qui donnera le temps à l'utilisateur d'enregistrer son travail en cours et d'arrêter le système en attendant le retour d'une ligne électrique stable.

9/ Il est recommandé de **« bloquer » une partie des droits du poste de travail**, comme l'installation de programmes. Dans ce cas, on considère qu'il existe un « Administrateur » du poste, qui dispose de toutes les fonctionnalités possibles sur le poste et un « Utilisateur » du poste, qui exécute les programmes mais ne peut pas en installer, limitant ainsi les risques de propagation involontaire de programmes malsains.

10/ A minima, les **données confidentielles présentes sur le poste doivent être chiffrées.** Si le poste est un poste critique, c'est l'ensemble du poste qui sera chiffré. Quant aux appareils mobiles (portables, tablettes), ils sont systématiquement chiffrés afin de protéger les données en cas de vol ou de perte de l'appareil.

11/ Les programmes installés sur le poste sont des programmes adaptés à l'usage du poste : la plupart des logiciels « gratuits » ne peuvent pas être utilisés dans un cadre professionnel, la licence en interdisant l'usage en milieu professionnel. D'autre part, dans de nombreux cas, ces logiciels « gratuits » sont peu adaptés, livrés sans garantie de fonctionnement, sans service, sans support et peuvent s'avérer plus bloquants qu'efficaces.

12/ Les personnes internes ou externes qui interviennent sur le système informatique doivent être connues et répertoriées. L'accès à un intervenant non habilité doit être interdit.



8

L'UTILISATION DES **OBJETS CONNECTÉS PERSONNELS** EN ENTREPRISE

Traditionnellement appelé « BYOD », de l'anglais « Bring your own device », signifiant « apportez vos appareils personnels ».

CE QU'IL FAUT RETENIR

- Dans la mesure du possible, le BYOD est une pratique à éviter.
- L'organisation peut tolérer l'usage d'objets numériques personnels en son sein, mais il est préférable d'isoler ces appareils du réseau professionnel.
- En cas de nécessité absolue de connexion au réseau, l'appareil doit être couvert par une suite de sécurité.
- Pas d'usage personnel d'un l'appareil professionnel.
- Il est possible de permettre / refuser l'accès au réseau de manière individuelle, en gérant chaque appareil qui se connecte (gestion des adresses MAC).

C'est la tolérance ou l'avantage qu'offre une entreprise permettant à un salarié de connecter un de ses équipements personnels (ordinateur portable, tablette, smartphone) au réseau de l'entreprise, soit à des fins personnelles, soit à des fins professionnelles.

Les smartphones sont très utilisés en entreprise et sont connectés au réseau wifi mis à disposition par l'entreprise. Ces appareils sont rarement protégés, les protections restant sommaires voire inexistantes.

Autoriser la connexion d'appareils personnels au réseau de l'entreprise impose de vérifier leur niveau de protection. De plus, ces appareils étant, par essence, propriété du salarié et non de l'entreprise, il n'est pas possible pour un employeur de vérifier quelles données sont présentes sur ces appareils.

Dans le cadre d'une telle tolérance, plusieurs règles sont de rigueur :

1/ Vérifier le **niveau de protection** de l'appareil.

2/ Engager avec l'ensemble du personnel une **démarche éthique**, allant jusqu'à la signature d'une charte de « bonne conduite ».

3/ Si l'usage est toléré pour **convenance personnelle** (appareil utilisable uniquement lors d'une pause ou dans certains lieux tels que réfectoire, cantine, salle de repos, espace fumeurs), il convient alors d'**isoler le réseau permettant la connexion wifi du reste du réseau de l'entreprise.**

4/ Si l'usage est toléré pour **convenance professionnelle** (appareil personnel utilisé en remplacement d'un matériel d'entreprise momentanément défectueux), il s'agira de **vérifier l'état général du poste** ainsi que son intégrité, avant de le connecter au réseau professionnel, et d'**imposer une sécurité sur ce poste**.

5/ Grand nombre d'applications installées sur les smartphones et tablettes récupèrent énormément de données : géolocalisation, accès aux données personnelles tels que numéros de téléphone, ensemble des contacts enregistrés dans l'appareil, appels téléphoniques, photos, habitudes de navigation… Une fois l'appareil connecté au réseau professionnel, d'autres données (celles de l'entreprise), peuvent devenir accessibles pour ces applications. Il est donc particulièrement important de **vérifier quelles applications sont installées** sur ces appareils et quels sont les droits que s'octroient ces applications.

6/ Il est nécessaire de **scinder partie personnelle et partie professionnelle.** Aucun courriel professionnel ne doit être transféré sur une adresse courriel personnelle. De même, l'appareil utilisé en entreprise ne doit pas être utilisé pour consulter des sites ou serveurs cloud personnels.

9

LA SÉCURISATION DU **RÉSEAU EXTERNE** DE L'ENTREPRISE

Tout comme l'entreprise dispose d'une adresse physique permettant à une personne mal intentionnée de s'y introduire, le réseau informatique de l'entreprise dispose aussi d'une adresse (par le biais de sa connexion internet) et cet accès externe permet de s'introduire « virtuellement » dans l'entreprise.

CE QU iL FAUT RETENiR

- L'accès au réseau interne depuis l'extérieur doit être protégé et surveillé.
- Les mots de passe par défaut du matériel informatique administrable doivent être changés.
- Les différents appareils doivent être connectés sur des plages d'adresses choisies et non pas «traditionnelles».
- Une analyse du trafic réseau doit être réalisée de manière régulière.
- Des solutions logicielles permettent de sélectionner « Qui » a accés à « Quoi » dans l'administration du réseau.

Le firewall : un mur de feu infranchissable ?

Aucun acteur de sécurité informatique digne de ce nom ne serait capable d'écrire noir sur blanc qu'un firewall est infranchissable. Ou bien ce serait un menteur !

Le firewall physique

(appareil analysant et régulant l'intégralité du trafic entrant et sortant de l'entreprise) reste cependant une protection efficace, dès lors que des règles strictes sont appliquées.

Traditionnellement complémentaire et plus efficace qu'un firewall intégré à un logiciel antivirus, le firewall physique, connecté en amont du réseau informatique, représente un bouclier entre le monde extérieur et l'entreprise. Associé à des services de réseaux virtuels, de zones sécurisées, zone DMZ, internet… l'accès n'en sera que plus difficile pour les cybercriminels.

Parallèlement à cette protection qui devrait être considérée comme indispensable et obligatoire dans toutes les entreprises, il convient de s'assurer qu'aucun matériel « administrable » à distance n'est resté dans sa configuration d'origine : les mots de passe et protocoles d'accès doivent être verrouillés.

Traditionnellement, les réseaux informatiques sont par défaut sur des plages d'adresses IP très courantes (192.168.1.xxx). Cela équivaut à un mot de passe de type « 1234 » : trop évident, trop facile. Le réseau doit être installé sur des plages d'adresses IP différentes.

Enfin, il convient de surveiller de manière régulière les remontées d'informations des firewalls (logs), qui sont un bon indicateur du nombre de tentatives faites pour entrer sur le réseau d'une entreprise et éventuellement découvrir par quel biais. En effet, la question n'est pas de vérifier si une tentative d'attaque a eu lieu, car c'est quasiment une certitude, mais plutôt de vérifier comment ont réagi les systèmes de sécurité mis en place.

10

NE PAS LAISSER DE **TRACE**

En agissant comme agiraient les cybercriminels (laisser le moins de traces possibles), l'environnement numérique est sécurisé.

CE QU iL FAUT RETENiR

- Nettoyage régulier, automatiquement ou manuellement, des cookies, historique de navigation, fichiers temporaires.
- Pas de mémorisation de mots de passe.
- Réduction du nombre de plugins installés.
- S'il existe, utilisation du navigateur fourni par la suite de sécurité.

1/ Il est conseillé de **vider l'historique** des navigateurs internet.

2/ Les navigateurs internet ne doivent pas être autorisés à mémoriser **les mots de passe**.

3/ Lors de sessions de navigation sur internet, il est préférable de choisir le **mode navigation privée**.

4/ Aucun fichier contenant vos mots de passe ne doit être stocké sur le poste de travail.

5/ Il est possible d'automatiser les tâches de suppression des **fichiers temporaires** : cette règle se doit d'être appliquée.

6/ Le **chiffrement** et la **protection** par mot de passe des documents sensibles doivent être appliqués, après avoir pris soin de réaliser une sauvegarde externalisée du document original non chiffré.

7/ Il n'est pas conseillé d'autoriser les sites internet à vous pister : il convient pour cela de vider systématiquement « **le cache** » du navigateur, et même mieux, d'activer la suppression automatique du cache et des **cookies** lors de la fermeture du navigateur.

8/ Il est important de choisir une version optimale et sécurisée d'un **navigateur** plutôt que des navigateurs récents, alternatifs, dont la sécurité est quelquefois laissée pour compte.

9/ Le nombre de **plugins** installés sur un poste doit être réduit au strict minimum.

11

BIEN CHOISIR SES PARTENAIRES

En dehors de l'entreprise elle-même, le prestataire informatique (ou service informatique interne s'il existe), est celui qui va détenir l'ensemble des informations liées à une structure informatique. Quelquefois, il disposera également de l'ensemble ou d'une partie des identifiants et mots de passe. Il est donc important de s'appuyer sur un partenaire de confiance.

CE QU'IL FAUT RETENIR

- Le prestataire informatique peut accéder à vos ressources informatiques : il doit être de confiance.
- Votre relation doit reposer sur une confiance réciproque.
- Il doit disposer de qualifications : choisissez un spécialiste, pas un amateur éclairé, passionné, ou un simple vendeur !
- Il doit être couvert par une assurance RC Professionnelle et pouvoir en apporter la preuve.

Dans la cadre d'un partenariat avec un prestataire

Il est important voire obligatoire, de vérifier que son niveau de sécurité est important : il doit avoir intégré l'ensemble des dispositions de ce guide ! Pour maintenir ce niveau d'exigence, le partenaire sérieux investit dans la formation et le suivi de ses compétences. Il a sélectionné des technologies et méthodes qui vont garantir le bon fonctionnement de votre informatique.

Il va détenir l'ensemble des informations de vos équipements numériques. S'il est victime d'une attaque majeure, vos données nécessaires à la maintenance, stockées chez ce prestataire pourraient devenir exposées. Il doit donc répondre à l'ensemble des critères de sécurité que vous avez définis. En matière de sécurité, le cordonnier ne peut être le plus mal chaussé !

Un partenaire de confiance :

A l'ère du cloud et des services en ligne, la proximité est toujours d'actualité : le prestataire doit être à vos côtés et en mesure de vous accompagner en toutes circonstances.

Le prestataire qui gère vos infrastructures numériques dispose très souvent d'un accès en télémaintenance sur l'ensemble de votre parc informatique. Il a donc accès à l'intégralité des données d'une entreprise. Dans ce cadre, un prestataire sera donc choisi avec le plus grand soin. Un contrat de confidentialité peut (doit) exister entre vous et lui.

Certains prestataires sont affiliés à des réseaux professionnels. C'est un gage de qualité et de confiance, ces réseaux imposant à leurs affiliés des compétences techniques et proposant régulièrement des formations techniques certifiantes, liées aux services informatiques. Privilégiez donc un acteur dont les compétences sont reconnues et validées par ses pairs. Ces investissements sont la garantie d'un prestataire efficace, qui place son client au centre de ses préoccupations. Il est à privilégier à un intermédiaire « de commerce », qui ne vous apportera qu'un prix, sans valeur.

Enfin, il doit disposer d'une assurance de type responsabilité professionnelle. Exigez-en une preuve.

12

DIRECTIVE RGPD

(Règlement Général sur la Protection des données)

Détermination des niveaux de risque et mise en œuvre des mesures de sécurité appropriées : des obligations structurantes de la mise en conformité avec le RGPD.

CE QU iL FAUT RETENiR

- Cette directive OBLIGATOIRE relative à la protection des données peut être « lourde » à intégrer dans les entreprises.
- Elle impose la mise en œuvre de multiples sécurités dans l'entreprise : c'est le côté positif !
- Les amendes administratives pour faute à la directive RGDP sont importantes : 20 millions d'Euros, ou 4 % du C.A + réparation / dédommagement qui peuvent être exigés par les parties concernées.

La sécurité des données personnelles est un élément central du **plan de conformité que toute entreprise doit mettre en place afin d'anticiper l'application à compter du 25 mai 2018** du Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (**RGPD**).

Le renforcement des obligations relatives à la sécurité des données correspond à une volonté des autorités de réduire le nombre d'incidents de sécurité donnant lieu à la diffusion de données personnelles au préjudice des personnes physiques concernées et tout particulièrement de leur vie privée.

La consultation des dernières sanctions prononcées par la CNIL montre d'ailleurs qu'il s'agit d'une priorité pour l'autorité française de protection des données personnelles. La dernière en date a été l'occasion de voir prononcer, pour la première fois, une amende de 40.000 Euros pour violation de données. La CNIL s'est appuyée de manière inédite sur les nouvelles règles issues de la loi République numérique entrée en vigueur en novembre 2016. Avant cette loi, seul un avertissement pouvait être prononcé.

Les obligations issues du RGPD en matière de sécurité des données :

Il faut d'abord préciser que le RGPD repose sur une logique de responsabilisation et de transparence (principe dit d' « accountability [1] »). En matière de sécurité des données, ce principe impose aux entreprises de mettre en œuvre par elles-mêmes des mécanismes et des procédures internes permettant de démonter le respect des règles relatives à la protection et à la sécurité des données.

Le RGPD prévoit une obligation de garantir la sécurité des données personnelles par la mise en place de mesures adéquates sur un plan technique et organisationnel, par exemple, la pseudonymisation ou le chiffrement des données. En pratique, il s'agit de se prémunir contre trois types de situations : défaut de confidentialité (accès non autorisé ou divulgation accidentelle de DCP), défaut de disponibilité (perte ou destruction de données résultant d'un acte malveillant ou d'un accident), ou défaut d'intégrité (altération des données résultant d'un acte malveillant ou d'un accident) (article 1§12 et Avis du Groupe de l'article 29/03/2014).

*(1) **L'accountability** désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.*

Cette première obligation n'est pas nouvelle. Le RGPD la renforce en précisant que les garanties doivent être intégrée par défaut au système d'information (principe du « Security by default »). De plus, il apporte quatre changements significatifs :

Premièrement,

pour chacun des traitements de données qu'elle opère, l'entreprise devra procéder à une évaluation des risques pour la vie privée. Il s'agit d'identifier, analyser, estimer, traiter les risques et organiser leur évaluation de manière régulière et ce, afin d'être en capacité de déterminer les mesures qui lui permettront de se conformer à l'obligation de garantir la sécurité des données. Dans certains cas, cette évaluation devra prendre la forme particulière d'une analyse d'impact et pourra conduire à une obligation pour l'entreprise de se rapprocher de la CNIL pour en quelque sorte, valider les mesures de sécurité requises pour des traitements spécifiques. L'analyse d'impact s'imposera par exemple pour les traitements de données sensibles[2] ou les traitements utilisés pour faire du profilage automatique.

Deuxièmement,

l'obligation de notification des violations de données personnelles : sauf à ce qu'elles ne représentent aucun risque pour les droits et libertés des personnes physique (en pratique, les hypothèses seront peu nombreuses), le responsable de traitement devra notifier à la CNIL, dans un délai de 72h, les mesures prises pour remédier à la violation, atténuer ses conséquence négatives et apporter des garanties quant au risque de répétition de l'incident. Il devra également fournir à l'autorité une description de la violation et des données concernées, les coordonnées du délégué à la protection des données ainsi qu'une description de l'impact probable de la violation.

Troisièmement,

il faut relever que la réputation de l'entreprise sera particulièrement exposée lorsque l'information de chacune des personnes concernées sera requise. Toutes les fois où la violation représentera un risque élevé pour leurs droits et libertés, l'entreprise sera en effet tenue, sauf exception, d'une obligation de communication aux personnes concernées.

Quatrièmement,

l'obligation de mettre en œuvre les mesures de sécurité appropriées pèse désormais directement sur le sous-traitant et non seulement sur son donneur d'ordre, le responsable de traitement. Le RGPD prévoit en effet une liste d'obligations qui doivent être obligatoirement prévues par le contrat entre le sous-traitant et son client. Entre autres, le sous-traitant aura la charge de prendre toutes mesures requises pour assurer la sécurité du traitement et d'aider le responsable du traitement à remplir ses obligations en matière de sécurité des données et de réalisation des analyses d'impact. Afin de limiter sa responsabilité, le sous-traitant devra être particulièrement attentif à la rédaction de ses contrats et à la documentation des échanges et recommandations adressées à ses clients.

Il est important de préciser que ces obligations relatives à la sécurité des données personnelles s'ajoutent à celles qui ont trait à la sécurisation du système d'information en tant que tel. Par exemple, en matière de contrat de maintenance informatique, le prestataire est tenu par une obligation de conseil et de mise en garde de son client. Une application particulière de cette obligation touche à la sécurité informatique et aux précautions qu'il doit inviter son client à prendre afin de limiter le risque d'incident de sécurité. L'étude de ce risque est compatible et peut être menée en parallèle de l'évaluation des risques sur la vie privée. A titre d'exemple, il est utile de se référer à la méthode EBIOS, méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Les recommandations pratiques de la CNIL

La CNIL a diffusé en octobre 2017 un guide dont l'objectif est d'accompagner les entreprises dans leur plan de mise en conformité avec les obligations de sécurité des données personnelles.

La CNIL propose une méthode en quatre volets à laquelle il est utile de se référer :

1/ Procéder au **recensement des traitements de données personnelles.** Afin de consolider cet inventaire, il est recommandé d'utiliser le modèle de registre de données proposé par la CNIL.

2/ Procéder à une **étude d'évaluation des risques** pour la vie privée engendrés par chacun des traitements recensés. A cette fin la CNIL met à disposition un questionnaire d'évaluation.

3/ Déterminer les mesures techniques et organisationnelles au vu des niveaux de risques. A cette fin la CNIL développe un volet de 17 fiches de recommandations concernant par exemple, la gestion des sites web, prestataires de maintenance ou sous-traitant.

4/ S'assurer de l'effectivité des mesures mises en place au moyen d'**audits de sécurité périodiques**.

*(2) **Donnée sensible** : Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.*

13

EN CAS DE **DOUTE**

Un poste informatique présente un comportement inhabituel, des éléments ont disparu ou sont apparus, le poste est très lent, des utilisateurs reçoivent des mails de votre part alors que vous n'avez rien expédié, vos identifiants sur un site ne vous permettent plus de vous connecter ?

CE QU'IL FAUT RETENIR

- Impératif d'alerter et de prévenir sans délai la hiérarchie et les services concernés.
- Ne pas essayer de se dépanner soi-même.
- En cas d'attaqué avérée : faire la déclaration d'incidents aux autorités.

Le premier conseil
en cas de doute est d'isoler le poste concerné en le déconnectant du réseau.

Il faut ensuite
procéder à une sauvegarde rapide du poste (pour une fois un support USB sera toléré) et uniquement des documents récents et importants, qui n'auraient pas encore fait l'objet de sauvegarde.

C'est seulement après cette étape que le poste pourra être éteint, de manière brutale (coupure par le bouton de mise en marche), et ne devra plus être rallumé, pour que d'éventuelles traces d'attaque ne soient pas souillées par une remise en route du poste.

Il convient ensuite d'avertir les responsables informatiques et, s'il existe, le prestataire, qui pourront procéder à l'analyse des données du disque et remettre en état le poste de travail, après s'être assurés que les sécurités sont opérationnelles.

Au retour en exploitation du poste
(ou avec un autre poste sain), il s'agit de modifier l'ensemble des mots de passe qui étaient en service sur le poste suspect.

Enfin, il s'agira de vérifier que les données restaurées sont exploitables (leur intégrité aura été vérifiée préalablement à leur restauration sur le poste).

Dans tous les cas
Ne tenter aucun dépannage par soi-même si les compétences nécessaires ne sont pas acquises.

La directive RGPD
impose la déclaration d'incident sous 72 heures aux autorités compétentes.

14

SE POSER LES **BONNES QUESTIONS**

Définir une politique de sécurité, c'est se poser les questions sur le niveau de probabilité de menaces, les risques encourus, et les comparer aux solutions mises en œuvre.

Complétez les tableaux p.31 en les remplissant avec la valeur « 1 » dans chaque case correspondant à votre cas (1 seule réponse par ligne), et reportez le total en dernière ligne.

Analyse de votre score.

Additionnez les résultats par colonnes des 3 tableaux.

Total tableaux 1+2+3	Total colone 1 + 2	
	Total colone 3 + 4	

Le total obtenu dans les 2 premières colonnes est **supérieur** au total obtenu dans les colonnes 3 et 4

Il est alors impératif que la question de la sécurité informatique soit étudiée rapidement et que des actions soient programmées pour restreindre les risques existants.

Le total obtenu dans les 2 premières colonnes est **quasi équivalent** au total obtenu dans les colonnes 3 et 4

Des solutions ont déjà été mises en place et il reste soit à les améliorer, soit à couvrir les risques qui n'ont pas encore été pris en compte.

Le total obtenu dans les colonnes 3 et 4 est **largement supérieur** au total obtenu dans les colonnes 1 et 2

Le risque numérique est déjà pris en compte et des solutions fortes existent. Un audit de sécurité confirmera ces bonnes pratiques.

1/ Niveau de probabilité de menaces

Niveau de **MENACE**	Menace **forte**	Menace **moyenne**	Menace **faible**	**Aucune menace** (ou improbable)
Intrusion physique dans les locaux et/ou incendie				
Panne disque dur				
Panne générale du système informatique				
Attaque cybercriminelle				
Total Tableau 1				

2/ Risques encourus

Niveau de **RISQUE**	Risque **fort**	Risque **moyen**	Risque **faible**	**Aucun risque** (ou improbable)
Vol du matériel informatique				
Perte définitive de données (Absence de sauvegarde externe)				
Impossibilité de poursuite rapide d'activité en cas de défaillance système				
Fuite de données confidentielles et/ou mise hors service du système (Absence de protection Firewall)				
Total tableau 2				

3/ Solutions mises en place

Niveau de **SÉCURITÉ**	**Aucune solution**	Solution **faible**	Solution **moyenne**	Solution **forte**
Protection des locaux (alarme, vidéo surveillance, accès difficile)				
Existence de sauvegardes fiables externalisées				
Plan de reprise d'activité				
Désactivation des accès Wifi				
Gestion de réseaux virtuels (Vlan)				
Connection de smartphones et appareils personnels				
Matériel mobile protégé par cryptage de données				
Protection contre les accès Internet externes				
Politique interne de l'entreprise en matière de sécurité				
Mots de passe forts				
Audits et contrôles de sécurité réguliers				
Personnel de l'entreprise formé sur la sécurité et informé des risques				
Prise en compte de la directive RGPD – Mai 2018				
Total Tableau 3				
Total tableaux 1+2+3				

Edition Novembre 2017
© FRP2i 2017
Création / Mise en page : pom'C - www.pom-c.fr