Sécurisez votre informatique dans le cadre du GDPR.

aruba
a Hewlett Packard Enterprise company

AC
Partenaire stratégique pour la gestion de votre infrastructure informatique.

Depuis des dizaînes d'années, AC investit dans la sécurité des infrastructures informatiques chez ses Clients.

Le GDPR (Règlement Général sur la Protection des Données) rend cette approche encore plus essentielle.

C'est l'occasion de parcourir 22 points sensibles liés :

- à la qualité des équipements informatiques en place ;
- aux logiciels de sécurité implantés ;
- aux services associés au maintien d'un haut niveau de disponibilité et de sécurité.

* Source: https://ec.europa.eu/info/law/law-topic/data-protection_fr

1. PROTÉGER L'ACCÈS AUX INFORMATIONS.

Choisir son Mot de passe.

Un **mot de passe judicieux** n'appartient pas au langage courant (les pirates utilisent ce que l'on appelle des fichiers «dictionnaires» pour parcourir rapidement des milliers de combinaisons composant des mots de passe possible) ni à votre sphère privée (nom des enfants, du chien...). Il faut définir son mot de passe **avec une longueur de minimum 8 lettres et chiffres** et surtout ne pas l'écrire dans un endroit accessible comme sur le clavier. L'idéal est d'arriver à un mot de passe n'ayant pas de sens, constitué de chiffres et de lettres, de majuscules et minuscules, de caractères exotiques. Pour le retenir, l'astuce est de trouver **un algorithme personnel**, comme par exemple prendre les consonnes d'un mot, ou une lettre sur deux, inverser les syllabes...

2. ACCÉDER À SES INFORMATIONS.

Définir des droits.

Dans l'environnement multi utilisateurs, la sécurité des ressources commence par **l'attribution étendue de droits et permissions aux utilisateurs**. Le système de fichiers est donc un élément fondamental et essentiel dans cette gestion de la sécurité et du partage des ressources.

3. EVITER LES VIRUS.

Le cas échéant, les éliminer.

Chaque PC et serveur sont livrés avec **un logiciel antivirus**. Il vérifie **en temps réel** l'ensemble des fichiers échangés. Le logiciel vérifie aussi les fichiers contenus sur le disque dur. La mise à jour de l'antivirus est réalisée chaque jour sur base des données récoltées par le serveur durant la nuit.

4. ALLÉGER SA BOÎTE AUX LETTRES.

Filtrer les spams.

La solution mise en place par AC se base sur le firewall. **Le logiciel implanté analyse les messages en fonction d'une base de données d'expéditeurs indésirables** mises à jour quotidiennement. Cette approche est complétée par une analyse du contenu des messages sur base de mots clés et du contexte. Enfin **une liste blanche ou noire** viendra finaliser l'étude.

5. ETRE VIGILANT.

Surveiller son comportement.

Méfiance et vigilance sont de rigueur dans la gestion des mails et téléchargements sur le Web. **Méfiez-vous des pièces jointes** et spécialement des fichiers attachés dont **les extensions** sont potentiellement **dangereuses** et source de déclenchement de virus. Ce sont notamment les exécutables (.exe), **les fichiers Visual Basic Script** (.vbs), **les screensaver** (.scr), **les fichiers batch** (.bat)... ou encore les pièces jointes comportant plusieurs extensions. Prudence aussi avant de communiquer votre adresse mail. **Veillez à protéger votre confidentialité** et celle de vos correspondants dans tous les échanges sur Internet.

6. DÉFINIR SA POLITIQUE D'ACCÈS À INTERNET.

Etablir un code de conduite.

AC propose un firewall qui gère la partie **« web filtering » capable de limiter en souplesse l'accès à la toile en respectant les impératifs de chaque organisation**. La qualité du filtrage dépend de la faculté d'appréhender les contenus du Web et de les classer correctement. L'outil proposé par AC référencie plus d'un milliard de pages Web et plusieurs millions d'URL. Les sites sont repris dans des catégories thématiques et sont mis à jour quotidiennement. L'idée du filtrage poursuit plusieurs objectifs. AC offre des solutions testées qui permettent de traduire en langage technique la politique que chaque commune ou syndicat veut suivre.

7. UTILISER UNE INFRASTRUCTURE DE QUALITÉ.

Utiliser le know how de AC.

Le métier d'AC est de **fournir et de maintenir une infrastructure informatique et de télécommunication ouverte** vers des services extérieurs et vers Internet.
Pour rendre cette installation **sûre et fiable**, AC possède et multiplie une somme de connaissances, de développements et d'expériences, qu'elle partage avec les communes.

8. UTILISER L'INFRASTRUCTURE.

Sauver les informations sur le serveur.

Les utilisateurs travaillant en réseau enregistrent naturellement leurs données sur le serveur. Ils profitent ainsi de la **procédure automatique de sauvegarde des données du serveur**.

9. VEILLER À L'ENVIRONNEMENT.

Ne rien laisser au hasard.

Les équipements seront **installés dans des locaux sûrs** dont l'accès est limité aux seules personnes responsables. Les objets étrangers à l'informatique ou générant de la poussière (découpeuse, déchiqueteuse...) seront écartés. **Un coffre ignifuge** pouvant contenir les cassettes et disques durs de sauvegarde sera installé dans un local distant.

10. MAXIMISER « L'UPTIME » DES SERVEURS.

Dédoubler les composants clés.

Pour assurer **un taux de disponibilité élevé**, la redondance de certains composants est assurée : **technologie RAID** pour les disques, **configuration d'un hot spare, dédoublement du système d'aération et d'alimentation**. Ces composants sont **hot swap** c'est-à-dire qu'ils peuvent être enlevés et branchés sans arrêter le système.

11. PROFITER DES RÉSEAUX.

Organiser le trafic.

En pratique, ce qu'on appelle les LAN (Local Area Network) ou réseaux locaux sont de moins en moins... locaux ! En effet ils connectent (par exemple par fibre optique) des sites disséminés sur le territoire communal. Dans certains cas, ils permettent l'accès à des équipements sans fils. Le type d'informations qui transitent par ces réseaux est aussi de plus en plus varié : données, voix, vidéosurveillance... Dans ce contexte, AC favorise le choix **de switches intelligents qui peuvent être gérés à distance. A partir d'un même réseau physique plusieurs réseaux virtuels sont programmés de manière à faire circuler différents types de données de façon sécurisée** à chaque fois sur un canal différent (un Vlan).

12. SE PROTÉGER DU MONDE EXTÉRIEUR.

Configurer des pare-feu.

AC installe **un firewall dédié** et au niveau du router de connexion à Internet.

13. PERMETTRE DES ACCÈS À DISTANCE.

Les contrôler minutieusement.

Le router met **le réseau informatique en contact avec l'extérieur** (des fournisseurs par exemple qui proposent de faire du support à distance) dont il faut strictement **contrôler les accès**. Les sécurités implantées par AC sont primordiales pour **se protéger d'une intrusion**. Exemples au niveau du router : connaissance du Numéro ISDN, vérification de l'adresse IP de l'appelant, mot de passe, fonction «call back».

14. RÉALISER UNE INSTALLATION ÉLECTRIQUE DE QUALITÉ.

Prévoir les coupures de courant.

L'alimentation électrique, particulièrement celle des serveurs est **déterminante pour la sécurité des personnes et la fiabilité des équipements**. L'installation est confiée à un électricien professionnel. Les équipements informatiques ne peuvent **assurer une parfaite disponibilité** que s'ils sont protégés des risques inhérents aux perturbations électriques aléatoires présentes sur le réseau de distribution d'énergie. Face à ces perturbations d'origines diverses, AC propose une gamme complète d'**UPS (alimentation sur batteries)**. Ces UPS sont équipés d'une carte réseau qui permet de les monitorer à distance et de faire remonter des alertes le cas échéant. Enfin ils sont équipés d'une sonde de température pour prévenir de toutes hausses anormales ce celle-ci.

15. ETRE MOBILE, SE CONNECTER SANS FIL, À L'INTÉRIEUR COMME À L'EXTÉRIEUR DE LA COMMUNE.

Accéder à ses informations en étant mobile.

AC apporte une attention particulière à **la sécurité d'accès mobile**, par charte de sécurité pour les accès « public ».

16. BÉTONNER SON MOT DE PASSE.

Opter pour un One Time Password.

Le principe du **mot de passe unique** (One Time Password ou OTP) permet qu'un nouveau mot de passe soit utilisé à chaque nouvelle connexion. Celui-ci est généré automatiquement soit par **un digipass**, soit via une application sur votre smartphone (affichage d'une série de 6 chiffres différents à chaque demande). Ce principe relève considérablement le niveau de sécurité (le mot de passe est utilisé une seule fois) et de simplicité (le mot de passe est calculé par l'ordinateur et non pas choisi par l'utilisateur). La validité limitée dans le temps du code chiffré rend le digipass bien plus sûr qu'un code d'accès classique. En outre, personne ne peut s'identifier sans connaître le code PIN. Il faut donc veiller à toujours conserver le digipass et le code PIN séparément.

17. PRÉVOIR LE PIRE PAR UN BACKUP ON LINE ET OFF LINE.

Anticiper la perte de données / un virus (encryptions des données).

Les disques durs USB installés par AC permettent de **stocker jusque 8 TBytes sur un seul disque.Une sauvegarde complète des données du serveur** (fichiers et messagerie) est réalisée chaque nuit. Dans le cadre du contrat de service AC prend soin de vérifier si celle-ci s'est bien déroulée.

18. PRÉVOIR L'INCIDENT MAJEUR.

Adopter la règle 3-2-1.

Les bonnes pratiques préconisent la présence des données avec **3 copies** (la production, sa copie et son backup), sur **2 types de supports** (disques internes au serveur + tape / disque USB) et avec **1 copie hors site**.

19. IMAGINER L'INCIDENT MAJEUR.

Réaliser des images fidèles des serveurs.

AC configure des utilitaires qui réalisent chaque nuit la création **d'images complètes des serveurs**. En cas d'incident majeur, **le temps de restauration du serveur sera réduit**.

20. GÉRER LES PROBLÈMES.

Les confier à AC.

L'helpdesk d'AC réceptionne **par email ou téléphone** les questions posées par l'utilisateur ou le responsable informatique. **Une réponse est apportée dans les plus brefs délais**. C'est le client qui décide du niveau de support : garantie du constructeur, extension de garantie, contrat de maintenance AC. C'est aussi le client qui décide de faire appel aux prestations en régie plutôt qu'aux forfaits. Ces contrats sont ouverts pour les équipements loués ou achetés. Au-delà du contrat de maintenance hardware, AC offre un contrat de services. Celui-ci va couvrir : l'intervention après réparation afin de reconfigurer les équipements, la couverture du système d'exploitation, la vérification de certains équipements chaque nuit, la création d'images des disques afin de diminuer les temps d'immobilisation, la création d'images personnalisées dynamiques en cas de configuration hors standard, l'établissement d'un compte-rendu hebdomadaire des incidents.

21. GÉRER LES INCIDENTS.

Les résoudre avant qu'ils ne surviennent.

La procédure **«auditeur»** établit un **inventaire du matériel connecté au réseau, des versions logicielles et versions anti-virus utilisées**. Elle vérifie encore **les capacités** des disques du serveur ou **le bon déroulement** des sauvegardes. Des écarts par rapport au standard sont identifiés par des codes de couleur facilement identifiables (vert, orange, rouge). Ce type de rapport est analysé chaque jour par AC
et mis à disposition du responsable informatique sur le site Web de AC.

22. NE PAS DONNER UNE DEUXIÈME VIE À VOS INFORMATIONS.

Détruire les données.

Lorsque le matériel est remplacé, **AC détruit les données contenues sur les serveurs**.

HELPDESK

GÉRER LES PROBLÈMES. Les confier à AC. 20

AUDITEUR

ANTICIPER LES INCIDENTS. Les résoudre avant qu'ils ne surviennent. 21

6 DÉFINIR UNE POLITIQUE D'ACCÈS À INTERNET. Établir un code de conduite.

16 BÉTONNER LES MOTS DE PASSE. Opter pour un One Time Password.

15 ÊTRE MOBILE. Accéder à ses informations à distance.

PROTÉGER L'ACCÈS AUX INFORMATIONS. Choisir son mot de passe. 1

EVITER LES VIRUS. Le cas échéant, les éliminer. 3

ETRE VIGILANT. Surveiller son comportement. 5

PROFITER DES RÉSEAUX. Organiser le trafic des données. 11

4 ALLÉGER SA BOÎTE AUX LETTRES. Filtrer les spams.

12 SE PROTÉGER DU MONDE EXTÉRIEUR. Configurer des pare-feu.

13 PERMETTRE DES ACCÈS À DISTANCE. Les contrôler minutieusement.

ÊTRE MOBILE. Accéder à ses informations à distance. 15

14 RÉALISER UNE INSTALLATION ÉLECTRIQUE DE QUALITÉ. Prévoir les coupures de courant.

UTILISER UNE INFRASTRUCTURE DE QUALITÉ. Utiliser le know-how de AC. 7

VEILLER À L'ENVIRONNEMENT. Ne rien laisser au hasard. 9

22 NE PAS DONNER UNE DEUXIÈME VIE AUX INFORMATIONS. Détruire les données.

DONNÉES

2 ACCÉDER À SES INFORMATIONS. Définir des droits.

MAXIMISER « L'UPTIME » DES SERVEURS. Dédoubler les composants clés. 10

8 UTILISER L'INFRASTRUCTURE. Sauver les informations sur le serveur.

IMAGINER L'INCIDENT MAJEUR. Réaliser des images fidèles des serveurs. 19

17 PRÉVOIR LE PIRE. Anticiper la perte de données.

18 PRÉVOIR L'INCIDENT MAJEUR. Adopter la règle 3-2-1.

AC

SIÈGE SOCIAL
1 rue Nicolas Simmer
L-2538 Luxembourg

CENTRE
DE COORDINATION
Brussels Airport Area
Excelsiorlaan 85
B-1930 Zaventem

Tél. + 32 2 725 69 30
info@aclux.lu

AC
Partenaire stratégique pour la gestion de votre infrastructure et informatique.

aruba
a Hewlett Packard Enterprise company

Source: https://ec.europa.eu/info/law/law-topic/data-protection_fr