La sécurité informatique appliquée aux cabinets d'avocats

Antoine BON - Lionel VEST – Romain WINCZEWSKI
Avocats au Barreau de Strasbourg
Membres fondateurs de l'association CYBERTRON

Plan d’intervention

1. La sécurité numérique : une obligation déontologique
2. Le diagnostic et l’identification des traitements
3. Les bonnes pratiques de sécurité informatique
4. Les logiciels libres, un atout de sécurité

La sécurité numérique :
Une obligation déontologique

Art. 3 de la loi 2016-1547

Les avocats proposent à leur clientèle une relation numérique dans un format garantissant l'interopérabilité de l'ensemble des échanges

Les avocats peuvent proposer des services en ligne

La sécurité numérique : Une obligation déontologique

Art. 66-5 du décret 71-1130

En toutes matières, que ce soit dans le domaine du conseil ou dans celui de la défense, les consultations adressées par un avocat à son client ou destinées à celui-ci, les correspondances échangées entre le client et son avocat, entre l'avocat et ses confrères à l'exception pour ces dernières de celles portant la mention " officielle ", les notes d'entretien et, plus généralement, toutes les pièces du dossier sont couvertes par le secret professionnel.

Le secret professionnel ne concerne pas que les correspondances entre l'avocat et son client. Il s'étend à toutes les pièces du dossier

La sécurité numérique : Une obligation déontologique

Art. 4 du décret n°2005-790

Sous réserve des strictes exigences de sa propre défense devant toute juridiction et des cas de déclaration ou de révélation prévues ou autorisées par la loi, l'avocat ne commet, en toute matière, aucune divulgation contrevenant au secret professionnel.

Respecter le secret professionnel implique de maitriser ses flux de données

La sécurité numérique : Une obligation déontologique

Art. 226-13 du Code Pénal

> *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.*

La sécurité numérique : Une obligation déontologique

Les avocats sont également soumis :

- Au RGPD entré en application le 25/05/2018
- A la loi pour la confiance sur l’économie numérique du 21/06/2004
- A la loi informatique et libertés du 06/01/1978

La sécurité numérique : Une obligation déontologique

Respecter le secret professionnel implique de ne pas utiliser :

- *Des services qui ne garantissent pas la confidentialité des données*
  Cela implique de décortiquer les conditions générales des services, notamment gratuits, que vous utilisez

- *Des services d'hébergement américains, car le Cloud Act et le Patriot Act permettent aux autorités américaines de récupérer les données d'une personne, y compris si celle-ci est de nationalité étrangère, et y compris si les données sont stockées sur un territoire étranger par une société américaine.*

Cela exclut de facto les services : GMAIL, GOOGLE AGENDA, GOOGLE DRIVE, MICROSOFT OUTLOOK 360, AMAZON AZURE, HOTMAIL, YAHOO MAIL, WHATSAPP, ONE DRIVE, MICROSOFT TEAMS.

La sécurité numérique : Une obligation déontologique

3. LES COMMUNICATIONS AVEC AVEC LES CLIENTS

Protégez vos courriels

L'article 34 de la *Loi concernant le cadre juridique des technologies de l'information*[11] impose l'obligation de protéger l'information confidentielle à moins que le client n'en relève l'avocat par écrit. Ainsi, non seulement l'avocat doit-il protéger l'information, il doit convenir des moyens pour ce faire avec le client. Les modalités de protection de vos courriels devraient être proportionnelles à la confidentialité de l'information qui y est contenue. Il est possible de concevoir certains cas dans lesquels de l'information confidentielle sera acheminée dans le corps du courriel avec le consentement du client.

Par contre, plus généralement, l'information confidentielle devra être colligée au sein d'une pièce jointe qui sera protégée. Un simple mot de passe peut être suffisant alors que parfois, il faudra privilégier le *chiffrement*[12] de la pièce jointe[13], celui du courriel entier[14] ou celui du canal de communication[15].

Pour en connaître davantage sur la sécurité des courriels, nous vous invitons à consulter les articles se retrouvant dans la note ci-jointe[16].

Par ailleurs, les clients devraient être avisés du fait que faire suivre une copie d'un courriel en lien avec votre relation avocat-client pourrait être interprété comme étant une renonciation au secret professionnel[17].

Les services de courriels gratuits

Les services de courriels gratuits (par ex.: Hotmail, Gmail ou Yahoo Mail) ne conviennent pas à la pratique du droit et mènent presque inévitablement à la violation d'obligations déontologiques de l'avocat. Comme le démontrent les termes et conditions d'usage de ces services, leur prix est en fait le secret professionnel de vos clients et votre vie privée[20].

Par conséquent, avant même de convenir avec votre client que vous communiquerez ensemble par voie de courriels, vous devriez aviser votre client que, selon le contrat intervenu avec son fournisseur de service de messagerie ou encore son employeur (dans le cas des adresses courriel professionnelles), il est possible que ces derniers se réservent le droit de consulter le contenu de leurs courriels, ceci ayant une incidence sur le respect de votre obligation au maintien du secret professionnel et de la confidentialité des communications[21].

Publicité par courriel

En vertu de la *Loi canadienne anti-pourriel*[22], un cabinet (ou l'un de ses employés/associés) serait autorisé à envoyer des messages électroniques commerciaux[23] à ses anciens clients pendant les deux ans qui suivent la fin du dernier mandat accompli pour ces derniers. Ces messages devraient alors respecter les exigences de forme et de contenu prévues dans la *Loi canadienne anti-pourriel* et dans le *Règlement sur la protection du commerce électro-*

Au Canada, il est expressément interdit pour les avocats de recourir à des messageries gratuites GMAIL, HOTMAIL, YAHOO MAIL

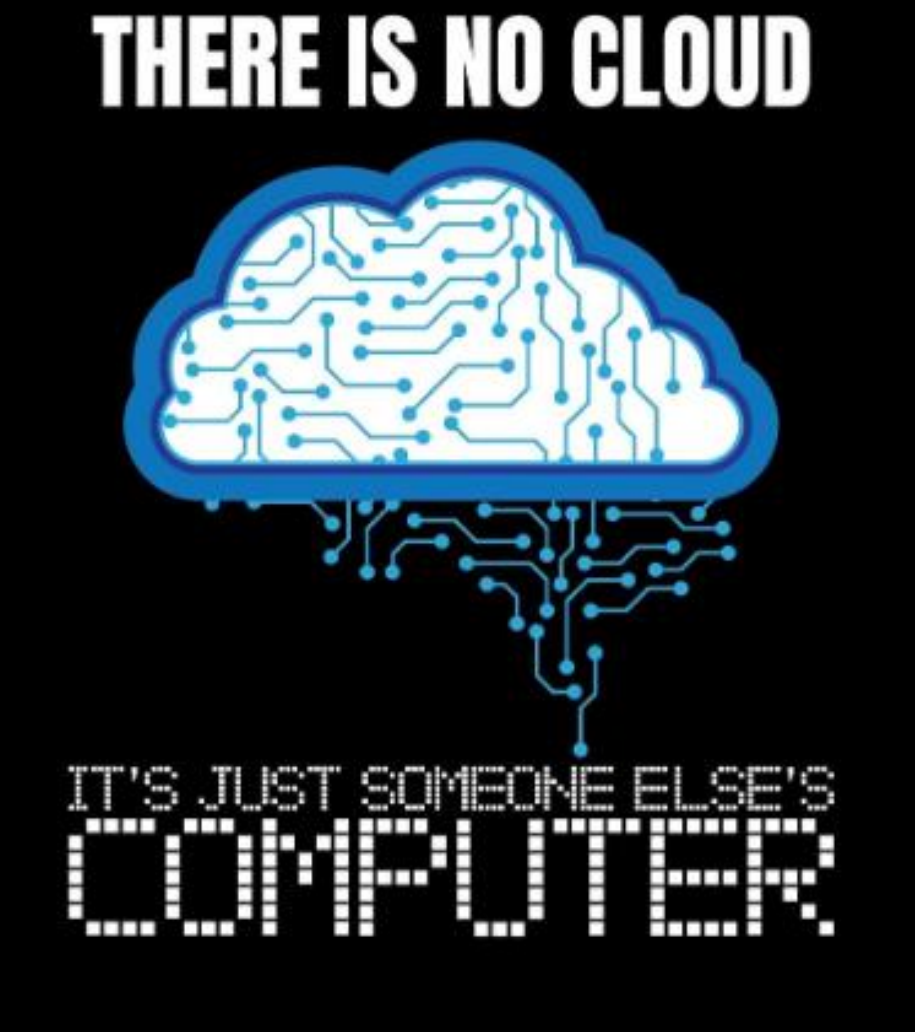
Pour traiter des dossiers sensibles, n'hésitez pas à fournir une boite mail sécurisée à votre client si celui-ci utilise GMAIL

Diagnostic
des traitements de données

Pour savoir si votre cabinet est en conformité, il faut :

- cartographier vos flux de données
- comprendre par où transitent vos données et celles de vos clients
- comprendre comment fonctionnent vos systèmes informatiques
- Mener une réflexion sur les outils de communication que vous utilisez (courriels, chats, système de visioconférence, cloud fichier, agenda)

Diagnostic
des traitements de données

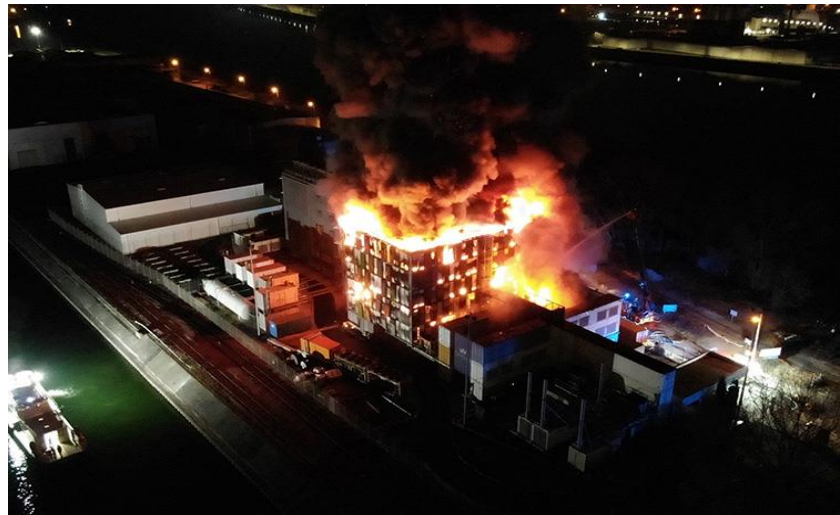


Où sont stockés vos fichiers ?
Où sont stockés vos courriels ?
Où sont stockées vos annuaires clients ?

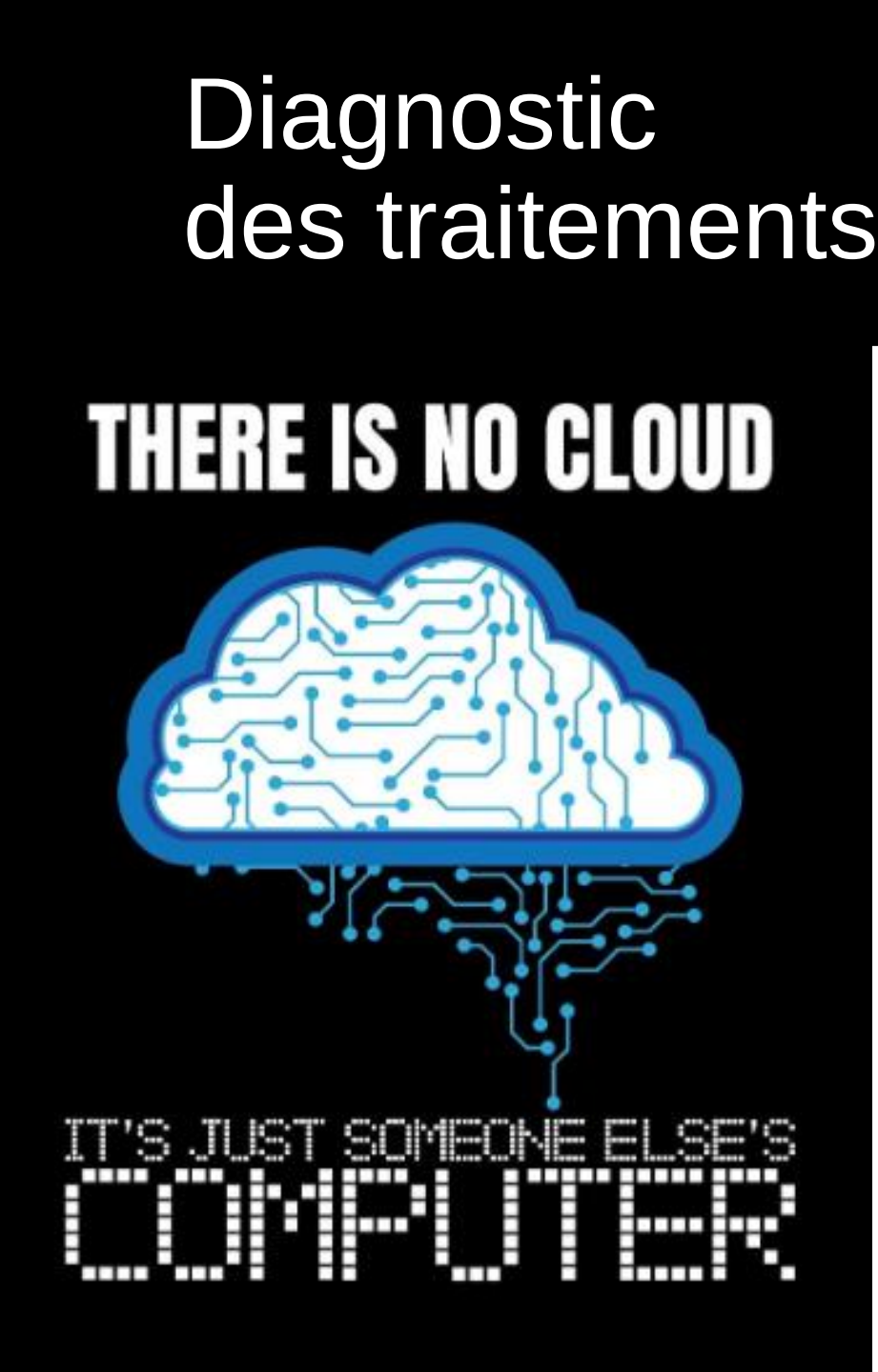
Le CLOUD n’est pas virtuel.
Les données ne sont pas évanescentes
Vous devez chercher à comprendre où sont stockés les fichiers

Incendie du DATACENTER
OVH CLOUD le 10/03/2021 :

De nombreuses entreprises ont réalisé que le cloud est quelque chose de bien concret en perdant définitivement leurs données lors de cet évènement



Diagnostic
des traitements de données



LA SOUVERAINETE NUMERIQUE

Gardez le contrôle sur vos données

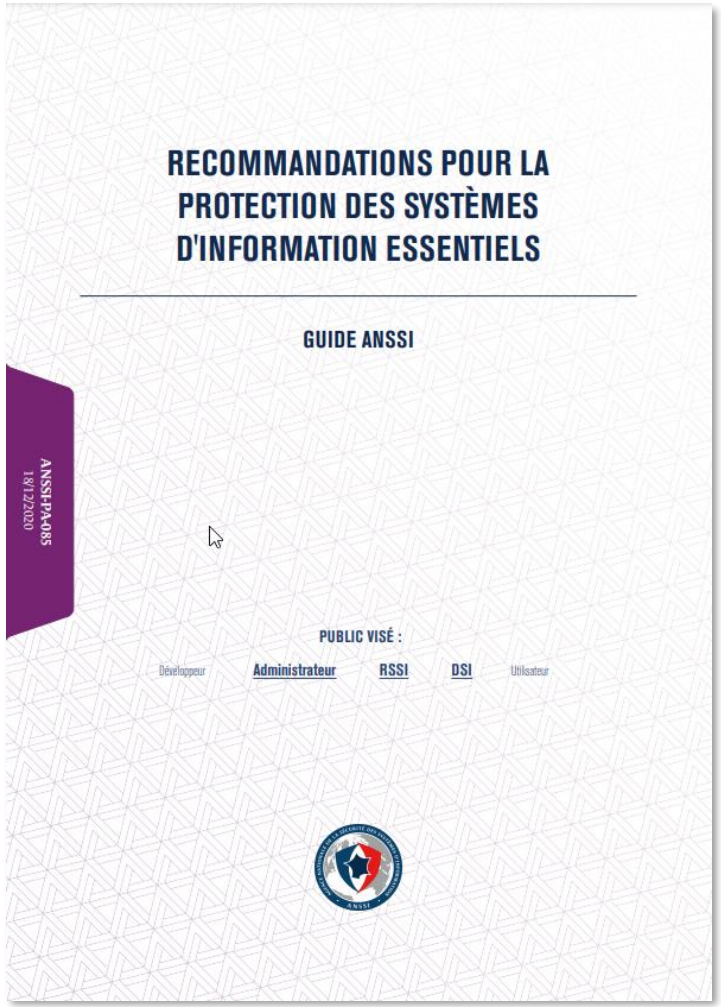
Hébergez votre propre cloud privé :

- Fichiers
- Courriels
- Annuaires clients
- Agendas
- Bases de données

Les bonnes pratiques de sécurité informatique

1. Gestion des utilisateurs
2. Gestion des mots de passe
3. Sécurité du poste de travail
4. Sauvegardes et plan de reprise de l’activité
5. Les équipements du cabinet
6. Sécurité du bâtiment
7. Lutte contre les virus et rançongiciels

Les bonnes pratiques de sécurité informatique



Un guide complet publié par l'ANSSI

https://www.ssi.gouv.fr/uploads/2020/12/guide_protection_des_systemes_essentiels.pdf

Les bonnes pratiques :
La gestion des utilisateurs

1. N’utilisez que des comptes individuels
2. Identifiez les ressources du cabinet
3. Ne donnez accès qu’aux ressources dont l’utilisateur a besoin
4. Désactivez les comptes inutilisés (anciens collaborateurs)
5. Confiez les accès administrateurs à au moins 2 personnes

Les bonnes pratiques :
La gestion des mots de passe

Ne pas utiliser :

- des noms propres
- des noms communs issus du dictionnaire,
- des citations de livres
- des paroles de chanson

y compris en les combinant

Les pirates disposent de « dictionnaires » très complets dans toutes les langues

- Avocat5521 ---> cracké en 1 seconde
- PabloEscobar5617 ---> cracké en 2 secondes
- ilétaitunpetitnavire ---> cracké en 5 secondes

Les bonnes pratiques :
La gestion des mots de passe

Mélangez majuscules, minuscules, chiffres et caractères spéciaux

Minuscules : 26 possibilités

LONGUEUR	POSSIBILITÉS	CRACK
6 caractères	26^6 = 308.915.776	< 1 seconde
9 caractères	26^9 = 5.429.503.678.976	< 22 minutes
10 caractères	26^10 = 141.167.095.653.376	< 9 heures
11 caractères	26^11 = 3.670.344.486.987.776	< 10 jours
12 caractères	26^12 = 95.428.956.661.682.176	< 276 jours

Minuscules et majuscules : 52 possibilités

LONGUEUR	POSSIBILITÉS	CRACK
6 caractères	52^6 = 19.770.609.664	< 4 secondes
9 caractères	52^9 = 2.779.905.883.635.712	< 8 jours
10 caractères	52^10 = 144.555.105.949.057.024	< 1 an
11 caractères	52^11 = 7.516.865.509.350.965.248	< 59 ans
12 caractères	52^12 = 390.877.006.486.250.192.896	< 3000 ans

Les bonnes pratiques :
La gestion des mots de passe

Votre mot de passe doit comprendre au moins 10 caractères

Minuscules, majuscules et chiffres
62 possibilités

LONGUEUR	POSSIBILITÉS	CRACK
6 caractères	62^6 = 56.800.235.584	< 14 minutes
9 caractères	62^9 = 13.537.086.546.263.552	< 39 jours
10 caractères	62^10 = 839.299.365.868.340.224	< 6 ans
11 caractères	62^11 = 52.036.560.683.837.093.888	< 412 ans
12 caractères	62^12 = 3.226.266.762.397.899.821.056	< 25.000 ans

Minuscules, majuscules, chiffres et spéciaux
156 possibilités

LONGUEUR	POSSIBILITÉS	CRACK
6 caractères	156^6 = 14.412.774.445.056	< 1 heure
9 caractères	156^9 = 54.716.887.507.601.719.296	< 433 ans
10 caractères	156^10 = 8.535.834.451.185.868.210.176	< 67.000 ans
11 caractères	156^11 = 1.331.590.174.384.995.440.787.456	< 10.000.000 ans
12 caractères	156^12 = 207.728.067.204.059.288.762.843.136	**> 1.000.000.000 ans**

Les bonnes pratiques :
La gestion des mots de passe

Ne jamais utiliser un même mot de passe sur plusieurs sites

- Une faille de sécurité sur un seul site compromettrait tous vos accès !
- Les pirates utilisent des robots qui testent les mot de passe volés sur les sites populaires

Ne notez pas vos mots de passe sur des post-its ou dans votre téléphone

- Ne notez jamais un mot de passe en clair
- Utilisez des logiciels de gestion de mot de passe (KEEPASS)

N’envoyez pas vos mots de passe par courriel

- Votre boite mail est la première cible des pirates
- Des logiciels scannent les boites mails à la recherche de mots de passe

Les bonnes pratiques :
La gestion des mots de passe

N’utilisez pas aveuglément la fonction « enregistrer votre mot de passe »

- Vous ne faites que reporter le risque sur le mot de passe de votre ordinateur

Activer l’authentification à deux facteurs (2FA) quand elle est disponible

- Evitez la validation par SMS
- Privilégiez les codes autogénérés (2FAS, AUTHY)

Modifiez toujours les mots de passe par défaut

- Surtout sur les box internet, routeurs et autres équipements réseau
- Evitez les identifiants évidents : admin / user / root

Les bonnes pratiques :
La gestion des mots de passe

Astuce simple :

- Inventez une phrase absurde : *mon lapin mange Strasbourg*
- Gardez les 2 premières lettres de chaque mot : molamaSt
- Mémorisez l'emplacement d'une majuscule : 2^{e} position ; mOlamaSt
- Mémorisez l'emplacement d'un caractère spécial : 4^{e} position $: mOl$amaSt
- Ajouter les deux premières lettres du site auquel vous vous connectez

Résultat unique pour linux.org : mOl$amaStli
Résultat unique pour avocat.fr : mOl$amaStav

Les bonnes pratiques :
La sécurité du poste de travail

Le risque le plus courant reste le vol de vos équipements

- Chiffrez vos disques : les données seront illisibles au prochain redémarrage

Ne laissez pas vos équipements allumés sans surveillance

- Fermez votre session en quittant votre bureau
- Eteignez votre poste de travail pendant la nuit

Assurez vous de bien purger vos disques en cas de revente

- Un simple formatage de disque ne suffit pas

Les bonnes pratiques :
La sécurité du poste de travail

Ne mélangez pas les usages

- Ne laissez pas vos enfants jouer avec votre ordinateur portable de travail
- N’installez pas des logiciels de loisir sur votre poste de travail
- N’autorisez pas vos collaborateurs à installer des logiciels sans votre accord

Ne connectez pas des clés USB dont vous ne connaissez pas l’origine

- Une attaque pirate connue consiste à abandonner une clé USB vérolée dans vos locaux

Installez régulièrement les mises à jour proposées

- Renouvelez le matériel obsolète qui ne reçoit plus de mises à jour

Les bonnes pratiques : Les sauvegardes

Effectuez des sauvegardes régulières, incrémentielles et automatiques

- Au moins une fois par jour, pendant la nuit
- Intégrez vos emails dans la sauvegarde
- N’utilisez pas des supports achetés le même jour

Ne stockez pas vos sauvegardes dans les mêmes locaux que vos données

- En cas de cambriolage ou d’incendie, la sauvegarde disparaitrait également
- Les données doivent exister en triple, dans au moins deux endroits différents

Les bonnes pratiques : Les sauvegardes

Vérifiez régulièrement vos sauvegardes

- Vérifiez que la sauvegarde quotidienne se déroule correctement
- Simulez régulièrement une restauration complète à partir de la sauvegarde

Appliquez à vos sauvegardes le même niveau de sécurité qu'à vos données

- Stockez les dans un endroit sécurisé
- Chiffrez les données
- N'allumez le serveur de sauvegarde que pendant le temps de la sauvegarde

Les bonnes pratiques :
Le plan de reprise d'activité

Objectif : faire face à un incident majeur

Recensez les risques :

- Cambriolage
- Incendie / dégât des eaux
- Corruption ou vol massif de données
- Arrêt complet des services de votre hébergeur
- Coupure durable de la connexion internet
- Disparition brutale d'un homme clé

Documentez

- Où sont les données ? Où sont les sauvegardes ? Qui y a accès ? Comment les restaurer ?
- Quelles sont les ressources nécessaires à l'activité (logiciels, documentation, serveurs informatiques)
- Qui sont les fournisseurs du cabinet ? Comment trouver leurs coordonnées ?
- Comment rétablir l'activité ? Sous quel délai ?
- Mise en place du télétravail comme mesure temporaire ? Avec quels outils ?

Les bonnes pratiques :
Les équipements du cabinet

Tout équipement connecté à votre réseau constitue une surface d'attaque

- **Photocopieurs** : attention aux boitiers qui remontent des informations de maintenance
- **Box internet** : changez les mots de passe par défaut. Fermez les ports inutiles
- **Sonnette avec visiophone** : isolez cet équipement de votre réseau informatique
- **Téléphonie par IP** : isolez la téléphonie de votre réseau informatique
- **Routeurs** : mettez en place un filtrage MAC pour interdire les équipements non autorisés
- **Wifi** : privilégiez des routeurs permettant de créer un réseau secondaire pour les clients
- **Objets connectés** (prises, interrupteurs, alarmes) : à éviter

Ces équipements sont souvent négligés :

- Pensez à les mettre à jour régulièrement
- Ne laissez pas les mots de passe par défaut
- Déconnectez les objets inutiles ou mettez les sur un réseau séparé

Les bonnes pratiques :
La sécurité du bâtiment

- Mettez en place des contrôles d’accès (clés, badges)
- Les serveurs de données et équipements réseaux ne doivent pas être installés dans des zones accessibles au public
- Seuls les utilisateurs autorisés doivent pouvoir accéder aux serveurs
- Menez une réflexion particulière sur les accès du personnel d’entretien
- Eteignez les postes de travail pendant la nuit
- Désactivez les prises Ethernet inutiles, surtout dans les espaces publics

Les bonnes pratiques : Lutte contre les virus

- 95% des infections proviennent d’emails infectés
- Ne jamais ouvrir une pièce jointe suspecte
- Identifiez les extensions de fichier douteuses : exe, pif, vbs, bat, docm
- Utilisez un service mail fournissant un antivirus côté serveur
- Privilégiez les systèmes d’exploitation Linux, peu ciblés
- Méfiez vous des antivirus gratuits qui sont parfois des virus

Les bonnes pratiques :
Lutte contre les rançongiciels

- Un double risque : perte et publication des données si non paiement de la rançon
- Les cabinets d’avocats sont particulièrement ciblés
- Un utilisateur ne doit avoir accès qu’aux dossiers qu’il traite (ce qui limite l’infection)
- Au quotidien, utilisez un compte utilisateur plutôt qu’un compte administrateur
- Les accès aux données doivent être coupés lorsque la poste de travail est inutilisé
- Mettez en place une surveillance du trafic réseau pour détecter les fuites de données
- Eteignez les postes de travail pendant la nuit ou les congés
- N’installez pas sur votre poste des logiciels étrangers à votre activité professionnelle

Une pratique libérale implique des outils libres

1. La liberté d’exercice, c’est la liberté de choisir et contrôler ses outils

1. exigez l’interopérabilité des données et des logiciels

Logiciel libre : définition

Ecosystème propriétaire : à vous de négocier vos droits

- durée d’engagement = prison
- standard fermés, absence de documentation = coût de sortie élevé
- rappelez vous que le prix augmentera avec le nombre d’utilisateurs (secrétaires, collaborateurs…)

Ecosystème libre : les 4 libertés garanties par la licence GPL

- l'utilisateur est libre de faire l'usage qu'il souhaite du logiciel, sans restriction, gratuitement
- l'utilisateur est libre de télécharger le code, le modifier ou l'améliorer.
- l'utilisateur est libre de redistribuer le logiciel original
- l'utilisateur est libre de distribuer les versions modifiées qu'il a créées.

Logiciels libres : avantages

1. **Interopérabilité** : les logiciels libres fonctionnent ensemble, facilement
2. **Evolutivité** : les logiciels libres peuvent être facilement améliorés
3. **Sécurité** : l'identification des problèmes est facilitée et leur résolution rapide
4. **Gratuité** : L'utilisation des logiciels libres est gratuite
5. **Documentation** : La standardisation réduit les coûts de maintenance
6. **Confiance** : Pas de commission pour les revendeurs = neutralité du conseil
7. **Communauté :** documentation, forums d'entraide, associations
8. **Engagement :** diffuser des valeurs de partage, de transparence, de liberté

Logiciels libres :
Un plus pour la sécurité ?

1. Lorsque le code est ouvert, il est davantage audité et donc plus sécurisé

2. Internet et les smartphones dépendent de la sécurité éprouvée de GNU/Linux
   (90 % des serveurs web de la planète, 99% des téléphones, 80% du hardware)

3. Avec un logiciel propriétaire, votre sécurité dépend d’un éditeur privé opaque
   Avec un logiciel libre, votre sécurité dépend d’une communauté transparente

Logiciels libres :
Un plus pour la sécurité ?

Réponse du Ministère des armées
publiée dans le JO Sénat du 09/01/2020 - page 138

éditeurs. Les objectifs de cette politique sont bien de favoriser l'interopérabilité par un recours aux standards, protocoles et formats d'échanges ouverts, de garantir la souveraineté (tant sur la confiance que la sécurisation) numérique, de maitriser et rationaliser les choix technologiques, de promouvoir le partage et la réutilisation des composants logiciels et d'exposer les ressources (données et services). Dans la continuité de ses directives pour le recours aux logiciels libres, le ministère mène actuellement une étude pour s'équiper d'un poste de travail entièrement libre (système d'exploitation et logiciels de bureautique), sur le périmètre de son réseau internet dédié. L'accès au code source des solutions numériques est effectivement un facteur facilitant la maîtrise de ces solutions, dans une optique tant de sécurité que de souveraineté numérique. Il convient cependant de noter que la disponibilité du code source

Un cabinet d’avocats libre : C’est possible !

1. Linux FEDORA ou UBUNTU pour remplacer Windows ou MacOs
2. FIREFOX ou BRAVE pour naviguer sur internet
3. LIBREOFFICE pour remplacer Word, Excel, Powerpoint
4. ROUNDCUBE pour remplacer GMAIL ou OUTLOOK
5. FULLCALENDAR pour remplacer GOOGLE AGENDA
6. SABREDAV pour remplacer GOOGLE DRIVE et GOOGLE CONTACTS
7. PDF ARRANGER ou OKULAR pour remplacer Adobe Acrobat
8. VLC MEDIA PLAYER pour lire les fichiers vidéo / audio
9. JITSI pour faire de la visioconférence
10. OPTIMUS pour héberger son cloud souverain et gérer son cabinet d’avocats

Un cabinet d'avocats libre : Quels obstacles ?

1. Tous les logiciels propriétaires n'ont pas d'équivalent libre
   mais tous les outils nécessaires à l'exercice de notre profession sont disponibles

1. RPVA : le CNB ne propose ni pilote, ni documentation, ni support Linux
   mais la communauté du libre a comblé ce manque : wiki.cybertron.fr
   le RPVA est désormais parfaitement fonctionnel sous Linux

3. INFOGREFFE ne fournit son outil de signature électronique que pour Windows
   il est cependant possible d'installer Windows et Linux sur la même machine
   autre alternative : signer ses PDF avec sa clé RPVA via LibreOffice sous Linux

Notre association CYBERTRON

- Une association à but non lucratif créée par des avocats
- Une équipe de bénévoles passionnés par l'informatique
- Un modèle économique basé sur les dons et subventions
- Des forums de discussion et d'entraide, des formations validantes
- Le développement d'outils libres et gratuits pour notre profession

- www.societe.ninja
- www.optimus-avocats.fr
- www.jurisprudence.ninja
- www.calcul.ninja

- https://www.cybertron.fr
- https://git.cybertron.fr
- https://wiki.cybertron.fr
- https://discord.cybertron.fr