CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

GUIDE PRATIQUE
LA SÉCURITÉ NUMÉRIQUE DU CABINET D'AVOCAT

1e ÉDITION
OCTOBRE 2023

1. PRENDRE CONSCIENCE DU RISQUE CYBER

SOMMAIRE

INTRODUCTION

La numérisation de la profession d'avocat s'accompagne de risques dits « cyber » qui ne cessent de s'intensifier. Les attaques, de plus en plus complexes, se multiplient et les Etats et les multinationales ne sont pas les seules victimes de ce phénomène.

Qu'ils soient de grande ou de petite taille, les cabinets d'avocats détiennent un grand nombre de données confidentielles très intéressantes pour les cyberattaquants. Toutes les données du cabinet font partie de son patrimoine immatériel (l'expression « or noir du XXIe siècle » est fréquemment utilisée à leur propos).

De l'individu isolé aux organisations, les attaques cybercriminelles sont perpétrées par une large palette d'acteurs aux motivations multiples.

Trois grands types de menaces sont identifiées :

- attaques à caractère lucratif – Ces attaques occupent le devant de la scène médiatique (ex : piratage des services informatiques du département de Seine-et-Marne le 6 novembre 2022) ;
- espionnages – Les campagnes d'espionnage constituent la principale finalité poursuivie par les attaquants avec les tentatives de déstabilisation et les actions de sabotage informatique (ex : logiciel espion Pegasus) ;
- influences et déstabilisations – Ces attaques visent généralement à déstabiliser des entreprises ou des Etats (ex : campagne Ghostwriter, attaques contre des infrastructures essentielles tels les hôpitaux).

Dans ces conditions, le **risque numérique** est un risque d'entreprise qui nécessite une approche holistique afin de s'assurer que la protection mise en œuvre est adéquate et le demeure dans le temps.

Une approche par les risques doit être adoptée au sein du cabinet, laquelle présente deux volets :

- un volet préventif, qui consiste à prévenir et anticiper une cyberattaque ;
- un volet curatif, qui consiste à traiter rapidement et efficacement le risque une fois celui-ci réalisé.

Quelle que soit sa taille, un cabinet d'avocats doit prendre conscience qu'il peut être à tout moment confronté à une attaque cybercriminelle qui constitue autant un défi informatique qu'organisationnel. Qu'il s'agisse, par exemple, de malveillance visant à la destruction de données ou d'espionnage économique et industriel, les conséquences des attaques informatiques sont désastreuses et peuvent mettre en jeu la pérennité du cabinet. Afin de pouvoir réagir efficacement et de limiter le plus possible les impacts en cas d'attaque, les cabinets doivent s'y préparer.

La cybersécurité fait partie d'une politique plus large de sécurité informatique du cabinet dont l'objectif est la gestion de tous les incidents numériques du cabinet (ex. incendie, inondation, défaillance d'un sous-traitant, cyberattaque etc.). Avant de poursuivre, il est important de distinguer ces deux notions.

La sécurité informatique désigne l'ensemble des mesures destinées à faire face aux risques susceptibles de porter atteinte à l'intégrité du système informatique d'une entreprise : incendie, inondation, défaillance d'un sous-traitant... Alors que la cybersécurité regroupe l'ensemble des mesures visant à protéger un système informatique face aux attaques informatiques malveillantes. La cybersécurité est une branche de la sécurité informatique et englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des informations (cf. norme ISO 27001), sensibles ou non, au sein d'une infrastructure numérique. Ce guide se concentrera uniquement sur la cybersécurité et les risques d'origine cyber.

La gestion du risque cyber n'est efficace que si le cabinet met en œuvre un socle de sécurité comprenant les bonnes pratiques, souvent présentées comme des mesures d'hygiène informatique. Ce socle est constitué d'un certain nombre de règles informatiques, mais également de mesures organisationnelles.

Toutes ces règles et mesures doivent être proportionnées et adaptées au cabinet, précisément à la sensibilité des informations qu'il traite et aux processus qu'il met en œuvre dans le cadre de son activité. Précisons que le mot « sensible » s'entend de manière large comme les données à protéger et susceptibles de compromettre l'activité du cabinet. Ces données sensibles peuvent être stratégiques, des données clients, des données organisationnelles, ou des catégories particulières de données comme des données de condamnations pénales et d'infractions au sens du Règlement général sur la protection des données (ci-après « RGPD »).

Plus qu'un guide de sécurité informatique, ce guide a vocation à faire prendre conscience aux cabinets d'avocats du risque cyber. En effet, la menace est réelle : l'attaque cyber n'est plus le fait d'un hacker isolé mais d'une industrie qui se spécialise et se structure avec de véritables chaînes de valeurs. Ceci explique l'augmentation croissante du nombre d'attaques.

L'idée de ce premier guide n'est pas de vous sensibiliser au risque cyber en général, mais au risque cyber de votre cabinet. C'est la raison pour laquelle ce guide commence par la cartographie des risques, car cette méthode a pour intérêt de personnaliser le risque, de faire prendre conscience du risque qui pèse sur votre cabinet (1).

Une fois le risque cabinet identifié, il s'agira de présenter un certain nombre de règles et de mesures qui constituent le socle de base que nous avons nommé de manière générique les mesures préventives (2). Ces mesures ont vocation à vous prémunir contre les attaques opportunistes qui constituent les attaques les plus fréquentes. Tout comme les cambrioleurs, un bon nombre de hackeurs s'attaquent en priorité aux cibles les plus faciles d'accès.

Enfin, ce guide présentera les premiers réflexes à avoir en cas de cyberattaque (3). Le nombre de cyberattaques étant croissant, il est probable que votre cabinet en soit un jour victime.

I. CARTOGRAPHIER LES RISQUES CYBER

L'un des objectifs de ce guide est de vous présenter, de manière sommaire, les grandes lignes de la méthode de cartographie des risques. Ce guide n'a pas pour but de vous présenter en détail cette méthode ni même de vous présenter différents scenarios.

Plus modestement, ce premier guide utilise cette méthode de cartographie pour vous faire prendre conscience, non pas du risque **cyber en général, mais du risque cyber auquel est confronté votre cabinet**.

Dans cette prise de conscience, vous serez amené à entrer dans la méthode de cartographie en vous posant une question simple : **quels sont les processus et quelles sont les données sans lesquelles mon cabinet ne peut pas fonctionner ?**

Tout dépend de votre activité.

Dans vos réflexions, gardez à l'esprit que le cabinet d'avocats peut être une cible de choix pour un attaquant qui aurait pour cible finale un client du cabinet.

I.1. POURQUOI RÉALISER UNE CARTOGRAPHIE ?

Cette cartographie permet de mieux connaitre votre cabinet : ses processus métiers et son système d'information, et ce, afin d'identifier les risques qui pèsent sur lui.

Sa réalisation est d'une importance majeure, car elle permet :

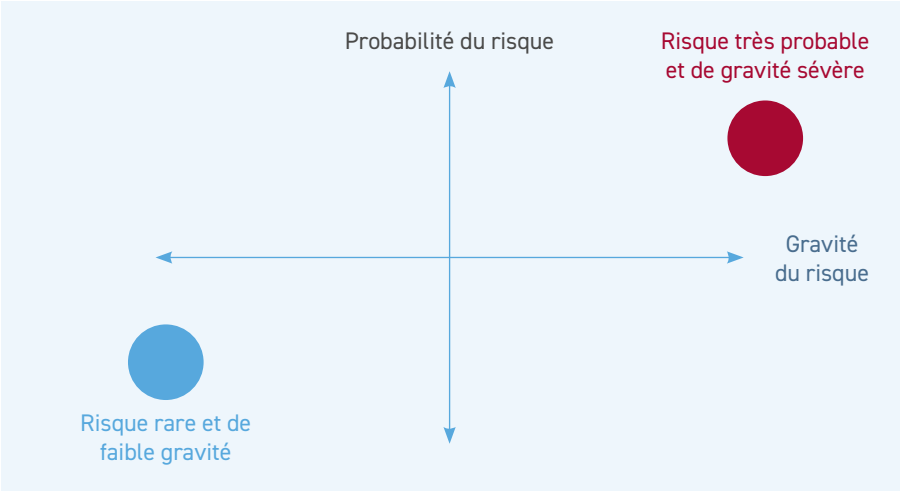
- de réaliser un audit de l'ensemble des traitements de données effectués par le cabinet ;
- de prendre conscience et de comprendre le risque cyber qui pèse sur les données dont le cabinet a la charge et pour lesquelles il est responsable d'une part, et sur les processus métiers primordiaux qui permettent au cabinet de mener à bien ses missions d'autre part ;
- de mettre en place un plan de traitement qui se traduit par la mise en œuvre d'un ensemble de mesures adaptées aux risques identifiés.

I.2. COMMENT CONSTRUIRE UNE CARTOGRAPHIE ?

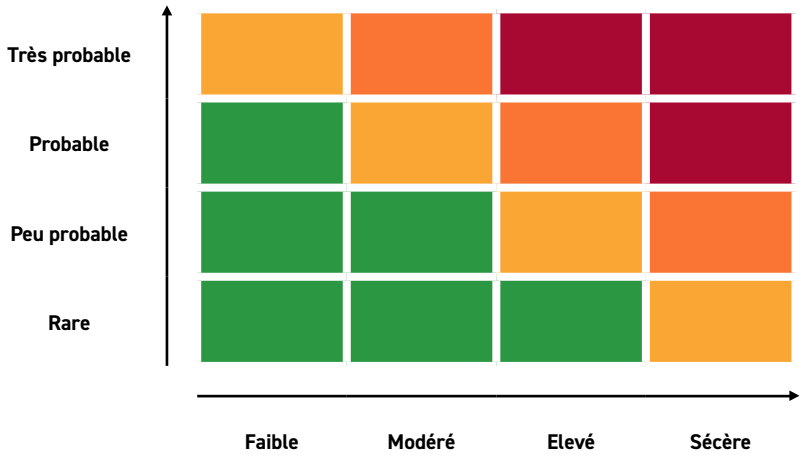
D'une manière générale, la construction d'une cartographie des risques permet d'avoir une vision globale des risques numériques pesant sur l'activité du cabinet, dont le risque cyber fait partie.

Une cartographie des risques est souvent présentée comme une matrice bidimensionnelle :

- un axe horizontal détaille le niveau de gravité de la survenance effective du risque (d'un niveau faible vers un niveau sévère) ;
- un axe vertical détaille la probabilité que ce risque survienne (d'une probabilité rare à une probabilité très probable).



La survenance de ces risques peut également être illustrée par une carte thermique. Des couleurs illustrent le niveau de gravité auquel les différentes activités du cabinet peuvent être exposées.



Les traitements qui apparaissent en rouge dans la cartographie ci-dessus nécessitent une attention toute particulière.

Les options de traitement à considérer sont :

- le refus du risque : consiste à décider de ne pas commencer ou poursuivre l'activité porteuse du risque ;
- la modification du risque : consiste à modifier la vraisemblance de l'occurrence d'un évènement (ou des conséquences), ou à modifier la gravité des conséquences. Il s'agit ici de mettre en œuvre des mesures de sécurité adaptées ;
- la prise du risque : par un choix éclairé ;
- le partage du risque : consiste à répartir les responsabilités entre différentes parties, en interne ou en externe.

La finalité de la cartographie des risques est la construction d'un plan de traitement des risques cyber qui se décompose en 4 temps :

1. Recensement des activités du cabinet et des catégories d'informations importantes traitées (cf. Les avocats et le Règlement général sur la protection des données (RGPD))
2. Identification des menaces cyber (atteinte à la disponibilité, à l'intégrité ou à la confidentialité) auxquelles ces activités et ces informations peuvent être confrontées, et évaluation de la gravité associée
3. Évaluation de la probabilité qu'une menace cyber touche les activités ou les données préalablement identifiées
4. Mise en place des options de traitement retenues

Le plan de traitement des risques est évolutif et doit être adapté en continu.

À ce stade, et sans entrer dans le détail de cette méthode qui fera l'objet d'un prochain guide, il convient de vous demander quels sont les processus et quelles sont les données sans lesquelles votre cabinet ne peut pas fonctionner ?

Par exemple, une activité tournée vers le judiciaire qui utilise beaucoup la communication électronique n'aura pas les mêmes réponses qu'un cabinet dont l'activité est plus tournée vers le conseil. La granularité peut être affinée en réfléchissant à votre structuration, à vos clients (avez-vous des clients célèbres, important par leur poids économique ou leur secteur d'activité, qui pourraient être la cible des hackeurs), à votre secteur d'activité (le risque n'est pas identique en droit de la famille, en droit de la propriété industrielle ou en droit pénal), etc.

POUR ALLER PLUS LOIN

Afin d'affiner votre cartographie des risques, il est essentiel d'établir une hiérarchie entre les données traitées par votre cabinet[1] :

- des données de vos clients couvertes par le secret professionnel :
  - des données sensibles au sens du RGPD et hautement personnelles au sens de la CNIL (données médicales sur l'état de santé, la vie personnelle, les finances, la situation économique, les rapports professionnels et la situation au travail, la religion, les opinions politiques, les opinions syndicales, etc.) ;
  - des données couvertes par le secret des affaires (ex. des informations sur une fusion-acquisition) ;
  - des données protégées par un droit de propriété industrielle (données de R&D, etc.) ;
  - des données sur des personnalités publiques ou des célébrités ;
  - des données stratégiques (fichiers clients, dossiers, pièces constitutives comme la pièce d'identité, les relevés, la déclaration d'impôt qui contient le numéro fiscal, le numéro de sécurité sociale, etc.).

1. Voir en ce sens : le-débat du 25 juin 2020 organisé par le CNB et consacré à la cybersécurité des cabinets d'avocats

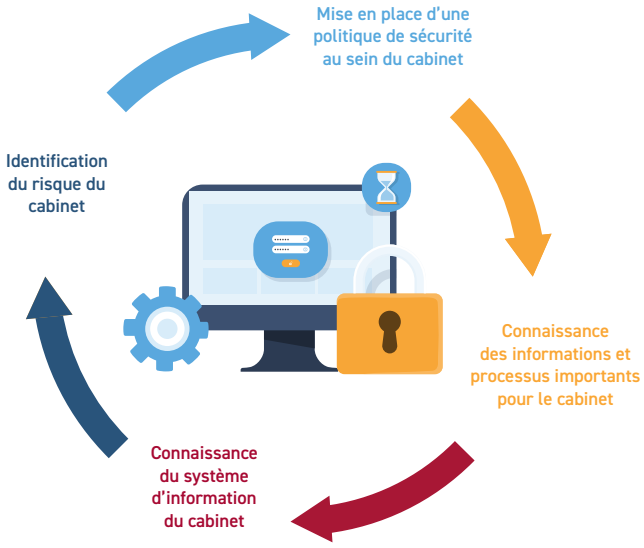
- des données relatives aux collaborateurs libéraux et salariés du cabinet, mais également les données relatives aux salariés du cabinet (assistant(e)s, juristes, etc.).
- des données fournisseurs (contrats de maintenance, contrats d'entretien, contrat de bail, contrat de location ou d'achat de photocopieur, de matériel informatique, etc.).
- des données relatives aux adversaires du client, ou encore aux représentants et mandataires du client personne morale, aux employés du client ou du groupe du client, aux employés ou représentants d'un partenaire commercial du client, aux clients du client (comme les consommateurs)...

Le risque numérique pesant sur les données ci-dessus n'est pas le même et dépend de la sensibilité (au sens large) des données.

Plus la donnée est sensible, plus la politique de sécurisation pesant sur le cabinet doit être rigoureuse, ce qui se traduit par une série des mesures parmi celles détaillées dans la suite de ce guide.

La gestion des risques du cabinet doit également intégrer les processus importants du cabinet (exemple : processus de facturation) et identifier les composants du système d'information (ex : un service, un serveur informatique, une application en mode SAAS...) qui supportent ces processus importants.

EN RÉSUMÉ SUR LA GESTION DE LA SÉCURITÉ DE L'INFORMATION



Références

ANSSI, La méthode EBIOS Risk Manager (2018)

ANSSI, Cartographie du système d'information (2018)

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

II. METTRE EN PLACE UN SOCLE DE SÉCURITÉ POUR PRÉVENIR LES ATTAQUES CYBER

Ce socle de sécurité s'applique plus généralement pour tout risque tenant à la sécurité informatique telle que nous l'avons défini dans l'introduction (ex. incendie).

Ce guide étant consacré à la cybersécurité, le socle de sécurité vous sera présenté sous l'angle de ce risque particulier qu'est l'attaque cyber.

FICHE 1
LA GESTION DE L'AUTHENTIFICATION

Comment authentifier les utilisateurs ?

La sécurisation du cabinet d'avocats passe par la mise en place de mécanismes d'authentification robuste.

L'authentification permet de prouver l'identité de l'utilisateur qui souhaite utiliser un outil, un logiciel ou encore un service, et de lui donner les accès nécessaires.

Plusieurs mécanismes permettant d'identifier un utilisateur peuvent être mis en place :

- un **facteur de connaissance** (« ce que l'on sait ») – ex. un mot de passe ;
- un **facteur de possession** (« ce que l'on a ») – ex. une clé contenant une puce (ex. clé Avocat) ;
- un **facteur inhérent** (une caractéristique propre à l'utilisateur) – ex. une empreinte digitale.

Pour assurer la sécurité des données du cabinet, vous devez mettre en place a minima, au moins l'un de ces facteurs d'authentification pour reconnaitre les utilisateurs et leur donner les accès nécessaires.

Toutefois, pour plus de sécurité, la CNIL conseille d'utiliser un mécanisme d'authentification multifacteur, c'est-à-dire un mécanisme qui repose sur au moins deux de ces trois facteurs.

Exemple d'authentification multifacteur : la clé avocat et le code PIN associé.

Comment mettre en place l'authentification au sein du cabinet ?

☐ Définir un identifiant et attribuer un compte par utilisateur

LES BONNES PRATIQUES :

- il est déconseillé de permettre l'utilisation de comptes partagés entre plusieurs membres du cabinet (et à plus forte raison avec des tiers). Une personne doit donc utiliser un compte qui lui est dédié.
- lors de l'attribution initiale du mot de passe (automatique ou par l'administrateur), l'utilisateur se doit de le modifier dès la première connexion afin qu'il soit le seul à en connaitre.

☐ **Limiter le nombre de tentatives d'accès à un compte** et bloquer temporairement l'accès à l'outil informatique une fois le nombre limite de tentatives atteint

POUR ALLER PLUS LOIN

Pour accentuer davantage la sécurité des authentifications à des services critiques, l'utilisateur peut choisir d'utiliser des navigateurs dédiés. Il sera ainsi possible sur ces navigateurs d'appliquer une configuration plus sécurisée et plus stricte que sur ceux réservés aux autres navigations.

Comment mettre en place une politique d'authentification par mot de passe efficace ?

L'authentification par mot de passe est fondée sur la connaissance d'un secret.

D'après une étude de Verizon de 2021, 81 % des notifications de violations de données mondiales seraient liées à une problématique de mots de passe. En France, environ 60 % des notifications reçues par la CNIL depuis le début de l'année 2021 sont liées à du piratage et un grand nombre aurait pu être évité par le respect de bonnes pratiques en matière de mots de passe.

Parmi les problématiques les plus constatées en matière de gestion des mots de passe se trouve la simplicité des mots de passe et l'absence de protections complémentaires de ceux-ci.

Afin de limiter au maximum les risques de compromission, il revient à chaque cabinet d'avocats d'adopter une politique d'authentification par mot de passe qui soit conforme aux recommandations de la CNIL. Il est à noter que si les clients du cabinet disposent d'un espace personnel numérique, cette politique doit également les concerner.

☑ Dans tous les cas, en matière de création et de renouvellement des mots de passe tout d'abord, il est important de veiller à :

☐ Utiliser un mot de passe complexe (entropie), de sorte qu'il soit impossible à deviner

BONNES PRATIQUES

- il est important que la longueur du mot de passe soit corrélée avec la criticité du service auquel il donne accès :
- en suivant les recommandations de la CNIL et de l'ANSSI, nous vous conseillons un minimum de 12 caractères
- un mot de passe complexe comporte des capitales, des minuscules, des chiffres et des caractères spéciaux.
- pour créer des mots de passe complexes, il est possible d'utiliser :
  - des moyens mnémotechniques (ex. ne conserver que les premières lettres des mots d'une phrase créée pour l'occasion ou utiliser des abréviations phonétiques)
  - des gestionnaires de mots de passe qui proposent, outre la fonction de stockage (cf. infra), de générer des mots de passe aléatoires, et pour certains d'entre eux d'avoir une estimation de leur entropie (degré de hasard ou de complexité du mot de passe)
- la CNIL propose sur son site d'accompagner les utilisateurs dans la génération d'un mot de passe solide mais également d'évaluer la robustesse du mot de passe choisi par eux.

☐ Utiliser un mot de passe différent pour chaque accès / service. Cette pratique permet en cas d'attaque d'un site ou de perte qu'un seul service seulement soit vulnérable

☐ Limiter le nombre de tentatives d'accès à un compte

☐ Privilégier, lorsque cela est possible, l'authentification multi-facteurs

☐ Changer régulièrement les mots de passe (entre 6 mois à 1 an)

- le nouveau mot de passe doit être entièrement renouvelé et notamment être le plus éloigné possible des anciens mots de passe
- le nouveau mot de passe généré doit correspondre aux critères de complexité précisés ci-dessus et, si possible, utiliser l'authentification multi-facteurs

☑ Recommandation : Pour faciliter le respect de ces règles, il est conseillé d'utiliser au sein du cabinet un logiciel de coffre-fort de mots de passe.

Les principaux avantages d'un coffre-fort de mots de passe sont :

- il génère aisément des mots de passe complexes et différents pour chaque service
- il n'est pas nécessaire de mémoriser ses mots de passe
- il permet le stockage sécurisé de ses mots de passe lesquels sont protégés par un mot de passe unique : il n'est alors nécessaire de retenir seulement un mot de passe complexe pour accéder à tous ses mots de passe
- il permet un changement facilité des mots de passe pour chaque service tout en s'assurant du respect du critère de complexité

QUEL LOGICIEL CHOISIR ?

Lors de la sélection d'un logiciel de coffre-fort de mots de passe, il est essentiel de tenir compte de plusieurs facteurs pour garantir la sécurité des informations sensibles. Voici quelques fonctions importantes à considérer :

- les fonctionnalités du logiciel (ex. pré-remplissage automatique, fonction d'audit des mots de passe, etc.)
- le mode de stockage du coffre-fort (dans le cloud ou en local sur votre ordinateur)
- la sécurité du logiciel (chiffrement, stockage, etc.)
- la sécurité du fournisseur
- la facilité d'utilisation du logiciel
- l'intégration du logiciel aux outils métiers
- l'authentification pour l'accès au logiciel de coffre-fort
- la maintenance
- le coût

L'ANSSI recommande le logiciel KeePass. KeePass est un logiciel open source qui permet de gérer différents mots de passe de manière sécurisée et chiffrée. Voir en ce sens la description du logiciel faite par l'ANSSI : https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/.

ⓘ POINT D'ATTENTION N° 1 : LE STOCKAGE UTILISÉ PAR LE LOGICIEL DE COFFRE-FORT :

Tout logiciel de coffre-fort de mots de passe contient un fichier « coffre-fort » où sont stockés de manière sécurisée tous vos mots de passe.

Le point d'attention porte sur l'endroit où est stocké ce coffre-fort :

- une première catégorie de logiciels vous propose de stocker ce coffre-fort dans le cloud : ce mode de stockage est un service offert par l'éditeur du logiciel
- une seconde catégorie de logiciels stocke ce coffre-fort en local sur le disque dur de votre ordinateur :
  - tel est le cas de la solution Keepass préconisée par l'ANSSI
  - **dans ce cas il est impératif d'assurer la sauvegarde sécurisée de votre coffre-fort** sous peine de perdre tous vos mots de passe (cf. point 2.4).

POINT D'ATTENTION N° 2 :

- ne pas laisser ses mots de passe visibles sur son espace de travail (ex. post-it)
- la solution consistant à utiliser un fichier bureautique de type Word ou Excel protégé par un mot de passe n'est pas recommandée car elle n'apporte pas un niveau de sécurité suffisant comparée à un logiciel de coffre-fort de mots de passe

POUR ALLER PLUS LOIN

Si malgré tout un risque de compromission du mot de passe survient, le cabinet doit, après en avoir été informé par l'utilisateur concerné :

- notifier à la CNIL dans un délai n'excédant pas 72h00,
- notifier aux personnes concernées dans les meilleurs délais si la compromission du mot de passe risque d'entraîner un risque élevé pour ces personnes,
- imposer au(x) membre(s) concerné(s) le changement de son mot de passe lors de sa prochaine connexion,
- recommander au(x) membre(s) concerné(s) de changer les mots de passe de ses autres services dans l'hypothèse où le même mot de passe y est utilisé.

EN RÉSUMÉ

- **privilégier l'utilisation d'un logiciel coffre-fort de mots de passe pour la création et le stockage de vos différents mots de passe**
- **privilégier, lorsque cela est possible, l'authentification multi-facteurs**

Références :

CNIL, Générer un mot de passe solide

CNIL, Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité (2022)

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

ANSSI, Etat de la menace informatique contre les cabinets d'avocats (2023)

ANSSI, Mesures cyber préventives prioritaires (2023)

ANSSI, Recommandations relatives à l'authentification multifacteur et aux mots de passe (2021)

FICHE 2
LA GESTION DES HABILITATIONS

Comment maitriser les accès aux outils informatiques du cabinet ?

Une des règles essentielles pour assurer la sécurité informatique du cabinet et des informations qu'il détient est de définir des profils d'habilitation au sein de l'entité.

L'objectif de ces règles est tout d'abord de permettre à chaque membre du cabinet d'obtenir uniquement les accès dont il a besoin. En cas d'attaque, ceci permet de limiter le risque au seul membre concerné et empêche sa propagation dans tout le système d'information du cabinet.

Ces règles doivent également permettre d'empêcher les utilisateurs d'installer de nouveaux logiciels via leur compte. Pour ce faire, il est nécessaire de créer deux comptes distincts :

- un compte sans privilège (compte utilisateur) pour la gestion des dossiers quotidiens
- un compte avec privilège (compte administrateur) auquel l'utilisateur n'a pas accès, pour l'installation et la désinstallation de logiciels

Il est également important de ne pas oublier de supprimer les autorisations d'accès obsolètes (tenant compte des départs du cabinet, ou des changements de service dans le cabinet) ou encore d'effacer les données présentes sur un outil numérique de travail préalablement à sa réaffectation à un autre utilisateur.

POUR ALLER PLUS LOIN

S'il le souhaite, le cabinet peut également réaliser une revue annuelle des habilitations pour s'assurer d'être à jour.

Références :

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

FICHE 3
LA SÉCURISATION DU MATÉRIEL INFORMATIQUE DU CABINET

Le cabinet possède de nombreux matériels (ordinateurs, téléphones, tablettes, imprimantes, objets connectés, routeurs réseau etc.) qui exploitent des données sensibles.

Ces outils constituent l'un des principaux points d'entrée des attaques cyber dans les systèmes d'information des cabinets d'avocats.

Afin d'assurer la sécurité numérique des processus métiers et des informations du cabinet, et y compris celles couvertes par le secret professionnel, il est essentiel de sécuriser informatiquement le cabinet.

En pratique, cette sécurisation informatique passe par une sécurisation des usages et des équipements informatiques de celui-ci : mises à jour, antivirus, sauvegardes, pare-feu, chiffrements, stricte séparation entre les usages, etc.

☐ Mettre à jour les logiciels et matériels informatiques du cabinet

Au sein du cabinet, chaque membre utilise quotidiennement différents types de logiciels (navigateur internet, logiciel de gestion du courrier, traitement de texte, visionneuse PDF, application de facturation, etc.) sur ses outils (ordinateurs, téléphones, tablettes, etc.).

Ces logiciels et outils numériques ont accès, et parfois détiennent, certaines données du cabinet.

Aussi, il est important que chaque membre veille à **appliquer les mises à jour de sécurité sur les matériels et les logiciels, dès lors que des correctifs sont proposés par l'éditeur.**

BONNES PRATIQUES

- si le logiciel le permet, il peut être utile pour le membre **d'activer l'option de téléchargement et d'installation automatique des mises à jour des outils et des logiciels les plus courants**. Dans cette situation, il doit tout de même **garder la possibilité d'effectuer des vérifications manuelles** si nécessaire ;
- si l'un des appareils ou logiciels ne peut plus être mis à jour, le membre concerné doit en informer la personne en charge de la sécurité dans le cabinet afin que celui-ci soit désinstallé et remplacé ;
- si le cabinet fait appel à des sous-traitants, il est recommandé au cabinet de s'assurer que ces derniers effectuent eux aussi la mise à jour de leurs propres outils et logiciels informatiques et de l'exiger dans les contrats de sous-traitance conclus avec eux.

☐ Effectuer des sauvegardes de données

Pour limiter au maximum les conséquences d'une attaque informatique sur l'activité et les clients du cabinet et permettre une restauration plus rapide des activités opérationnelles, il est important d'effectuer des sauvegardes régulières de données.

Sur la mise en place de sauvegardes cf. point 2.4.

☐ Installer un antivirus sur les outils du cabinet

Afin de se protéger des vulnérabilités, il est recommandé d'implémenter sur chaque outil informatique du cabinet, surtout ceux connectés à internet, un service de protection des menaces tel qu'un antivirus. Cet antivirus doit être déployé sur les ordinateurs, mais également sur les serveurs, les téléphones et les tablettes.

Il est important pour l'utilisateur de veiller à utiliser des antivirus mis à jour. En effet, si l'antivirus n'est pas à jour la protection offerte par celui-ci s'en trouvera restreinte.

☐ Installer un logiciel pare-feu sur les outils du cabinet

S'il n'est pas déjà intégré dans le système d'exploitation et dans une perspective de sécurisation toujours plus optimale, le cabinet peut également **installer sur les différents outils du cabinet un logiciel pare-feu.**

En pratique, ce logiciel protège principalement des attaques issues d'internet et permet de ralentir et/ou de limiter l'action d'une personne malveillante qui souhaiterait prendre la maîtrise du système d'information.

☐ Séparer ses usages informatiques

Pour augmenter significativement le niveau de sécurité de son cabinet, il est primordial pour le cabinet d'imposer une séparation stricte entre les usages et de proscrire ainsi aux membres l'usage d'outils personnels dans un but professionnel, et inversement.

L'interconnexion entre les outils présente un certain nombre de risques tels que l'exfiltration de données, l'atteinte à la disponibilité du système informatique ou des outils du cabinet, et plus globalement la violation de données protégées couvertes par le secret professionnel et/ou stratégiques.

BONNES PRATIQUES

Il est préconisé au cabinet d'interdire (par le biais de la charte informatique par exemple (cf. 2.8 sensibiliser et former les membres du cabinet) aux membres de :

- stocker les données professionnelles qu'il détient sur des sites de stockage personnel, et inversement ;
- utiliser sa messagerie personnelle dans un but professionnel ;
- transférer des messages entre ses messageries personnelles et professionnelles et d'utiliser des mots de passe identiques ;
- utiliser des services de stockage en ligne (cloud) personnels (niveau de sécurité moindre) à des fins professionnelles ;

- se connecter à des réseaux wifi inconnus ou publics, à moins d'être équipé d'un VPN lui permettant de chiffrer les données échangées ;
- et ce, afin d'éviter de rendre accessible les données protégées et stratégiques du cabinet et de mettre en danger leur confidentialité et/ou leur intégrité.

Afin d'orienter les membres dans leur utilisation, le cabinet peut également leur conseiller certaines bonnes pratiques.

Exemple : en cas d'urgence nécessitant l'utilisation de la messagerie personnelle à des fins professionnelles, le cabinet peut recommander aux membres le chiffrement systématique des messages et des pièces-jointes.

☐ Chiffrer les données protégées et les données stratégiques du cabinet

Les cabinets d'avocats possèdent de nombreuses données personnelles et stratégiques et les cyberattaquants en ont pleinement conscience.

Pour garantir la confidentialité des données de son cabinet, il peut donc être utile pour le cabinet d'utiliser des méthodes de chiffrement des données « sensibles » qu'ils possèdent et qui pourraient être dérobées ou auxquelles une personne malveillante pourrait accéder.

Techniquement, le chiffrement est une méthode qui consiste à protéger la confidentialité des données en les rendant illisibles par toute personne n'ayant pas en sa possession la clé de déchiffrement. Grâce à cette méthode, seules les personnes visées que sont les émetteurs et destinataires légitimes peuvent avoir accès aux données chiffrées.

A contrario, l'absence de chiffrement de bout en bout des données rend possible leur consultation en clair par un utilisateur, et compromet la protection du secret professionnel.

C'est généralement le cas des données stockées sur le cloud qui se trouvent généralement en clair et qui sont ainsi potentiellement lisibles.

BONNES PRATIQUES

Pour protéger la confidentialité des données des cabinets d'avocats, il est conseillé de :

- chiffrer les données, en transit et au repos, contenues sur les postes nomades (ordinateurs, téléphones, tablettes, etc.) et les supports amovibles avec un logiciel maîtrisé ;
- chiffrer les données sensibles avant de les communiquer, et ce quel que soit le moyen de communication utilisé (messagerie, messagerie instantanée, etc.) ;
- configurer un mot de passe de déchiffrement ;
- diversifier les secrets de chiffrement de manière segmentée (ex. par client, par affaire, ou encore par service) et de mettre en place une procédure de gestion de ses clés, celles-ci devant toujours être sauvegardées par le cabinet en cas d'oubli par l'un des utilisateurs

(!) POINT D'ATTENTION :

il est important de communiquer le mot de passe de déchiffrement par un autre moyen de communication que celui utilisé pour l'envoi des données.

POUR ALLER PLUS LOIN

La Commission Nationale de l'Informatique et des Libertés (ci-après « CNIL ») met également à disposition sur son site un tutoriel sur la méthode de chiffrement qui se trouve directement accessible via le lien suivant : Comment chiffrer ses documents et ses répertoires ? | CNIL

☐ Sécuriser le verrouillage et le déverrouillage des sessions

Sur chaque outil numérique du cabinet, qu'il soit fixe ou nomade, il est important de prévoir une procédure de verrouillage automatique de la session d'un membre à l'issue d'une courte période d'inactivité (inférieure à 5 minutes) et d'exiger un mot de passe pour le déverrouillage de celle-ci.

☐ Utiliser un filtre de confidentialité

Pour davantage de confidentialité, il est conseillé aux membres d'utiliser sur chacun de leurs outils informatiques à usage professionnel un filtre de confidentialité écran, notamment lorsque ceux-ci sont amenés à être en situation de nomadisme et qu'ils sont susceptibles d'utiliser leurs outils dans des lieux publics.

☐ Mettre en place l'impression sécurisée

Pour garantir la confidentialité des données au sein du cabinet, le cabinet peut également mettre en place l'impression dite sécurisée des imprimantes. Cette pratique permet de veiller à ce que les impressions effectuées sur les machines partagées ne soient ni visibles, ni accessibles par des tiers.

Cette pratique peut par exemple se matérialiser par l'exigence d'un code PIN confidentiel exigé avant l'impression sur la machine.

Références :

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

FICHE 4
LA SAUVEGARDE DES DONNÉES DU CABINET

La sauvegarde des données est une étape à ne pas négliger.

Les mesures de sécurité mises en place s'avèrent parfois insuffisantes pour faire face aux cyberattaques et la perte irréversible de données a des conséquences désastreuses sur l'activité du cabinet.

En cas d'incident majeur ou d'attaque, la mise en place d'une procédure de sauvegardes régulières permettra de restaurer les données perdues ou corrompues et de redémarrer plus rapidement l'activité du cabinet (en quelques jours au lieu de quelques semaines voire, dans le pire des cas, quelques mois).

Pour être en mesure de gérer la restauration des données altérées la procédure de sauvegarde doit être appliquée par l'ensemble des membres du cabinet (associés, collaborateurs, salariés du cabinet non-avocats).

Elle doit répondre à quatre questions :

- Quelles données doivent être sauvegardées ? Quelles sont les données vitales pour le cabinet ?
- A quelle fréquence les données doivent-elle être sauvegardées ?
- Sur quels supports les données doivent-elle être sauvegardées ?
- Comment récupérer les données sauvegardées ?

☐ Identifier les données à sauvegarder

La première étape de la procédure de sauvegarde consiste à identifier les groupes de données traitées et les hiérarchiser selon leur degré d'importance.

Les données identifiées comme indispensables à la continuité de l'activité du cabinet doivent pouvoir être récupérées rapidement en cas de cyberattaque.

Pour identifier ces données il est possible de se poser la question suivante : **quelles sont les données sans lesquelles l'activité du cabinet serait paralysée ?**

Il peut s'agir de fichiers clients, de dossiers clients, de dossiers de procédures mais également de données plus techniques comme la configuration du système informatique ou les fichiers de configuration des applications.

Dès lors que les différents groupes de données ont été identifiés il est recommandé de leur attribuer une procédure de sauvegarde appropriée à leur importance pour le cabinet.

☐ Diversifier les solutions de sauvegarde

Il est fortement recommandé de multiplier les solutions de sauvegarde.

L'ANSSI conseille d'appliquer la règle « 3-2-1 » :

- 3 copies de sauvegarde ;
- sur 2 supports différents ;
- dont 1 hors ligne.

Les données doivent être sauvegardées sur deux supports différents :

- une sauvegarde sur un support dématérialisé, en ligne ;
- une sauvegarde sur un support physique, hors ligne.

FOCUS SUR LA SAUVEGARDE EN LIGNE

Les sauvegardes en ligne sur des services en nuage possèdent l'avantage d'être simples d'utilisation et généralement peu coûteuses. Les données du cabinet sont confiées à un prestataire tiers qui se charge de les conserver de manière sécurisée.

La sauvegarde des données sur le cloud garanti leur accès à tout moment depuis n'importe quel ordinateur, tablette ou smartphone.

Confier ses données à un tiers n'est pas sans risques et ne doit pas contrevenir au secret professionnel des avocats. En effet, les solutions d'hébergement de données américaines sont soumises à la Foreign Intelligence Surveillance Act qui autorise les administrations américaines à collecter les données personnelles détenues par les personnes morales de droit américain.

Avant d'avoir recours à un service de sauvegarde il est recommandé de réaliser une analyse de risques et d'être vigilant dans le choix de son prestataire. Il est fréquent que les utilisateurs de ces solutions souffrent d'une insuffisance de transparence de la part des prestataires.

Si ces solutions sont faciles d'accès, généralement peu coûteuses et relativement simple à utiliser, leur connexion au réseau informatique les rend vulnérables face aux cyberattaques. Les cyberattaquants ont compris l'intérêt de verrouiller l'utilisation des sauvegardes de données des entreprises. En 2021, dans plus de 20% des cas des attaques par ransomware, les systèmes de sauvegarde ont été ciblés jusqu'à avoir été rendus inutilisables[2].

Cette information doit inciter les avocats à multiplier leurs supports de sauvegarde. Enregistrer les données sur un support physique, déconnecté du réseau internet, offre une sortie de secours en cas de verrouillage des données sauvées sur le cloud.

2. https://www.riskinsight-wavestone.com/2021/11/cyber-attaques-quels-risques-sur-les-sauvegardes-et-comment-sen-proteger/

FOCUS SUR LA SAUVEGARDE HORS LIGNE (OU SAUVEGARDE À FROID)

Les données sauvegardées sur des solutions en ligne étant exposées aux cyberattaques, il est opportun d'effectuer une deuxième sauvegarde des données sur un support physique hors ligne.

Plusieurs solutions existent :
- le disque dur externe ;
- un serveur installé dans le cabinet sur un réseau dédié ;
- un stockage sur bande ;
- un stockage cloud ;
- etc.

La sauvegarde de données sur un disque dur externe doit respecter quelques règles :
- le disque dur doit être chiffré ;
- le disque dur doit être déconnecté du système d'information à l'issue de la sauvegarde ;
- son usage doit être réservé à la sauvegarde des données du cabinet ;
- il ne doit pas être connecté à des postes extérieurs au cabinet ;
- Il est préconisé de ne pas laisser le disque dur dans les locaux du cabinet pour être en mesure de restaurer les données en cas de vol de matériel, d'incendie, etc.

Dès lors que les supports ont été sélectionnés il est nécessaire de déterminer la fréquence à laquelle les sauvegardes vont être réalisées.

☐ Définir la fréquence des sauvegardes

Une politique de sauvegarde est le premier rempart pour la résilience des systèmes d'information et constitue la première étape de la maîtrise des données.

C'est pourquoi il est indispensable de mettre en place des sauvegardes fréquentes.

La périodicité des sauvegardes dépend du groupe de données concerné. Plus les données sont importantes plus la fréquence des sauvegardes doit être élevée.

Les périodicités possibles

Quotidienne

Une sauvegarde quotidienne est définie comme une sauvegarde incrémentale déclenchée une fois par jour à heure fixe.

Hebdomadaire

Une sauvegarde hebdomadaire est définie comme une sauvegarde complète déclenchée une fois par semaine, le samedi à minuit de préférence.

Mensuelle

Une sauvegarde mensuelle est définie comme une sauvegarde complète déclenchée une fois par mois, le premier jour du mois à minuit de préférence.

La fréquence des sauvegardes se définit en fonction du volume de données produites

sur un temps donné. Par exemple, une sauvegarde mensuelle implique d'accepter une perte des données d'un mois.

Il est conseillé de mettre en place une procédure de sauvegarde quotidienne des données sur les deux supports sélectionnés, en ligne et hors ligne, pour vous assurer un redémarrage rapide de l'activité de votre cabinet en cas de cyberattaque.

Différents types de sauvegardes existent

Sauvegarde complète

Une sauvegarde complète est une image des données à l'instant où celle-ci est effectuée. Elle est auto suffisante pour la restauration en cas de nécessité.

Sauvegarde différentielle

Une sauvegarde différentielle est une sauvegarde qui ne prend que les modifications depuis la dernière bonne sauvegarde complète uniquement.

En cas de restauration, il faut d'abord restaurer la sauvegarde complète de référence et la sauvegarde différentielle du jour nécessaire.

Sauvegarde incrémentale

Une sauvegarde incrémentale est une sauvegarde qui ne prend que les modifications depuis la dernière sauvegarde complète et vérifiée.

Références :

ANSSI, Les règles d'or de la sauvegarde

ANSSI, Familles de produits

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

FICHE 5
LE NOMADISME

Le matériel informatique permet le travail en mobilité et dans les lieux publics (ordinateur portable, tablette, smartphone), ce qui accroit les risques de cyberattaques.

Pour faire face à l'accroissement des cybermenaces les avocats doivent adapter le niveau de sécurité de leurs appareils professionnels à cette nouvelle façon de travailler.

Il est de plus en plus fréquent que les avocats évoluent dans ces circonstances :

- travail dans les transports en communs ;
- travail dans des lieux publics ;
- travail à l'étranger.

Dans ces situations, les risques suivants sont accentués[3] :

- perte ou vol de matériel ;
- compromission du matériel ;
- compromission des informations contenues dans le matériel ;
- accès illégitime au système d'information de l'entité ;
- interception voire altération des informations.

La mise en place de certaines mesures permet de limiter les risques cyber accentués par le travail en mobilité

☐ Séparer ses usages informatiques

Il est primordial pour le cabinet d'imposer une séparation stricte entre les usages et de proscrire ainsi aux membres l'usage d'outils personnels dans un but professionnel, et inversement.

En effet, l'interconnexion entre les outils présente un certain nombre de risques tels que l'exfiltration de données, l'atteinte à la disponibilité du système informatique ou des outils du cabinet, et plus globalement la violation de données protégées couvertes par le secret professionnel.

☐ Sensibiliser les membres du cabinet sur le travail nomade (cf. partie 2.8.)

Dans un premier temps les collaborateurs du cabinet doivent être sensibilisés aux risques dont ils sont exposés dans les situations de mobilité. En matière de cybersécurité, la faille la plus importante est de nature humaine.

3. Voir en ce sens le guide de l'ANSSI « Recommandations sur le nomadisme numérique »

☐ Mettre en place des filtres de confidentialité sur ses écrans

Dans les lieux publics il est impératif d'équiper systématiquement son équipement informatique de filtres écran de confidentialité. Ce système physique permet de se protéger contre les regards des personnes indiscrètes.

Le *shoulder surfing*, signifiant littéralement « navigation par-dessus l'épaule » est une technique utilisée par certains malfaiteurs pour avoir accès aux données confidentielles appartenant à leurs victimes.

☐ Ne pas se connecter aux réseaux Wifi publics non sécurisés

Lors de leurs déplacements, personnels ou professionnels, il est fréquent que les avocats connectent leurs appareils informatiques à des réseaux Wifi publics non sécurisés pour économiser leur connexion en 4G ou 5G. Cette mauvaise habitude est à bannir.

Se connecter à un réseau Wifi non sécurisé comporte de nombreux risques. Si le point d'accès Wifi est mal configuré, ce qui est probable, les cyberattaquants auront la possibilité de voler les données stockées sur le matériel connecté.

☐ Chiffrer les données stockées sur le matériel informatique nomade

Le travail en mobilité conduit régulièrement à la perte ou au vol du matériel informatique. Ces évènements sont susceptibles de porter atteinte aux données qui y sont stockées.

Les données stockées dans le matériel nomade doivent impérativement être chiffrées afin de préserver leur confidentialité en cas de perte ou de vol. L'accès à l'ordinateur et au fichier contenant les données doivent être sécurisés par un mot de passe robuste.

Références :

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

FICHE 6
LA SÉCURISATION DES ÉCHANGES

UNE SÉCURITÉ TOUTE RELATIVE DES ÉCHANGES PAR EMAIL

Les emails sont un outil de communication incontournable, en témoignent les 333 milliards de mails échangés chaque jour[4].

L'email est l'instrument préféré des cyberattaquants car il constitue un point d'accès facile vers d'autres comptes et appareils de l'utilisateur.

Dans 90 % des cas, une cyberattaque commence par l'envoi d'un email[5].

La sécurisation de votre messagerie est une pièce maîtresse dans la politique de cybersécurité de votre cabinet.

L'email est un instrument simple de communication mais sa sécurité est toute relative.

En soi, un email n'est pas sécurisé.

La sécurité de l'email dépend deux éléments qui peuvent ou non se cumuler :

- la sécurité des connexions : elle est assurée par un protocole sécurisé (TLS) qui chiffre la connexion mais pas les messages. Sont ainsi sécurisées la connexion des usagers aux serveurs de messagerie et des serveurs de messagerie entre eux (serveurs d'envoi et serveurs de réception) ;
- la sécurité du contenu du message : le contenu du message n'étant pas sécurisé, il est lisible par toute personne qui parvient à l'intercepter. Ceci signifie que quand la sécurité des connexions est assurée, le contenu de l'email que vous envoyez ou que vous recevez ne l'est pas.

Si un cyberattaquant accède à votre boîte email, le contenu de tous vos emails (reçus et envoyés) est parfaitement lisible. C'est la raison pour laquelle le choix de votre mot de passe est crucial (cf. point 2.1).

Apparaît alors une autre faiblesse des emails, **l'impossibilité de s'assurer de l'identité de son émetteur.** Si vous recevez un message, dans la plupart des cas il est bien émis par la personne qu'elle prétend être, mais vous ne pouvez pas, à la seule lecture du message, vous en assurer à 100 %.

Trois types d'attaques exploitent cette dernière faiblesse des emails :

- **L'hameçonnage** (phishing en anglais) est l'une des attaques les plus employées par les cybercriminels :
  - cette technique vise à leurrer la victime dans le but de l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe, données bancaires) en se faisant passer pour une personne de confiance. C'est l'une des formes de cyberattaque les plus simples à réaliser pour les cybercriminels.
  - elle comporte trois éléments :

4. *Statistique publiée par Statista Research Department*
5. ANSSI, Panorama de la menace 2022

- elle est menée par la voie électronique
- l'attaquant prétend être une personne ou une organisation en qui la victime peut avoir confiance
- l'attaque vise à obtenir des informations personnelles sensibles.

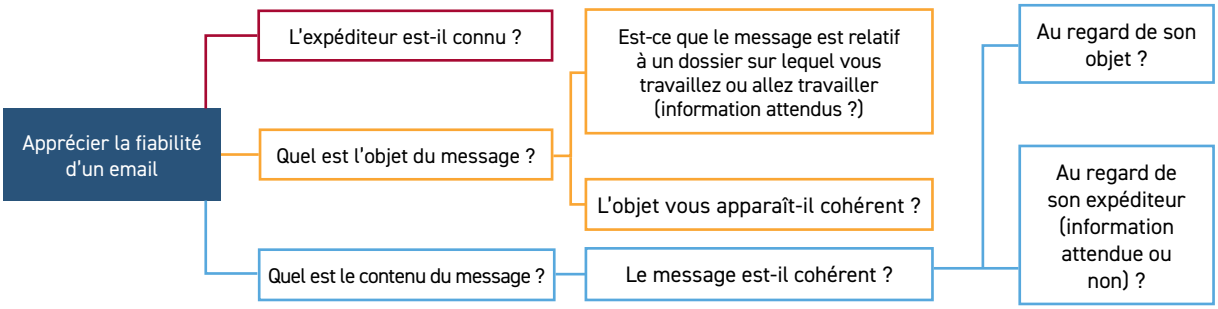
- **Le piratage de compte** désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime, comme un compte de messagerie email. Le piratage de compte peut avoir pour cause un mot de passe trop faible ou être la conséquence d'un hameçonnage.
- **L'arnaque au président** consiste pour les cybercriminels à se faire passer pour le dirigeant de l'entreprise. Le cybercriminel entre en contact avec l'un des collaborateurs de l'entreprise par email ou par téléphone. Après quelques échanges destinés à gagner la confiance de son interlocuteur, le cybercriminel convainc la victime d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant.

COMMENT APPRÉCIER LA FIABILITÉ D'UN EMAIL ?

La fiabilité d'un email se mesure par une analyse contextuelle :

- la personne émettrice : est-elle connue ou non ?
- l'objet du message : correspond-il à un dossier sur lequel vous travaillez ou allez travailler (information attendue) ? Sinon, l'objet vous apparaît-il cohérent ?
- le contenu du message : est-il cohérent au regard de l'émetteur et de son objet ?
  - doivent être considérées comme incohérentes toutes demandes de transmission de données confidentielles (mot de passe, coordonnées bancaires pour effectuer un virement, etc.) et ce quand bien même elles seraient reçues d'émetteurs connus
  - il convient également de prêter attention aux liens dans le contenu de l'email qui peuvent renvoyer vers des sites malveillants : le lien est-il cohérent avec l'émetteur du message ou son objet (ex. contrôle de l'adresse url du site) ?

IMAGE MENTALE POUR APPRÉCIER LA FIABILITÉ D'UN EMAIL



COMMENT APPRÉCIER LA FIABILITÉ D'UNE PIÈCE JOINTE ?

les pièces jointes sont particulièrement dangereuses car elles peuvent contenir un programme malveillant qui s'exécute à son ouverture pour endommager ou interrompre l'activité de votre ordinateur et, dans le pire des cas, de tout le système informatique du cabinet.

FOCUS SUR LES RANÇONGICIELS

L'ANSSI définit le rançongiciel comme un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Cette attaque consiste en l'envoi d'un logiciel malveillant (malware) qui chiffre l'ensemble des données stockées sur le réseau de la victime. Les cybercriminels demandent ensuite une rançon en échange de la clé de déchiffrement. Il existe des centaines de variantes de rançongiciels.

Ces dernières années, trois tendances illustrent les attaques par rançongiciels[6] :

- le ransomware-as-a-service (RaaS) : de plus en plus de rançongiciels sont rendus disponibles via des systèmes d'affiliation. Ceci illustre la professionnalisation des organisations cybercriminelles qui tendent à devenir des prestataires de services ;
- le Big Game Hunting : l'ANSSI a constaté une augmentation des attaques par rançongiciel des grosses entreprises et institutions publiques ;
- la double extorsion : les cybercriminels font pression sur leurs victimes en les menaçant de publier sur internet les données récupérées au cours de la cyberattaque.

Les attaques par rançongiciel peuvent être classées en trois catégories[7] :

- les campagnes d'attaques massives non ciblées ;
- les campagnes massives automatiques ;
- les attaques ciblées dites « Big Game Hunting » qui ciblent de grandes entreprises/institutions susceptibles de payer d'importantes sommes d'argent.

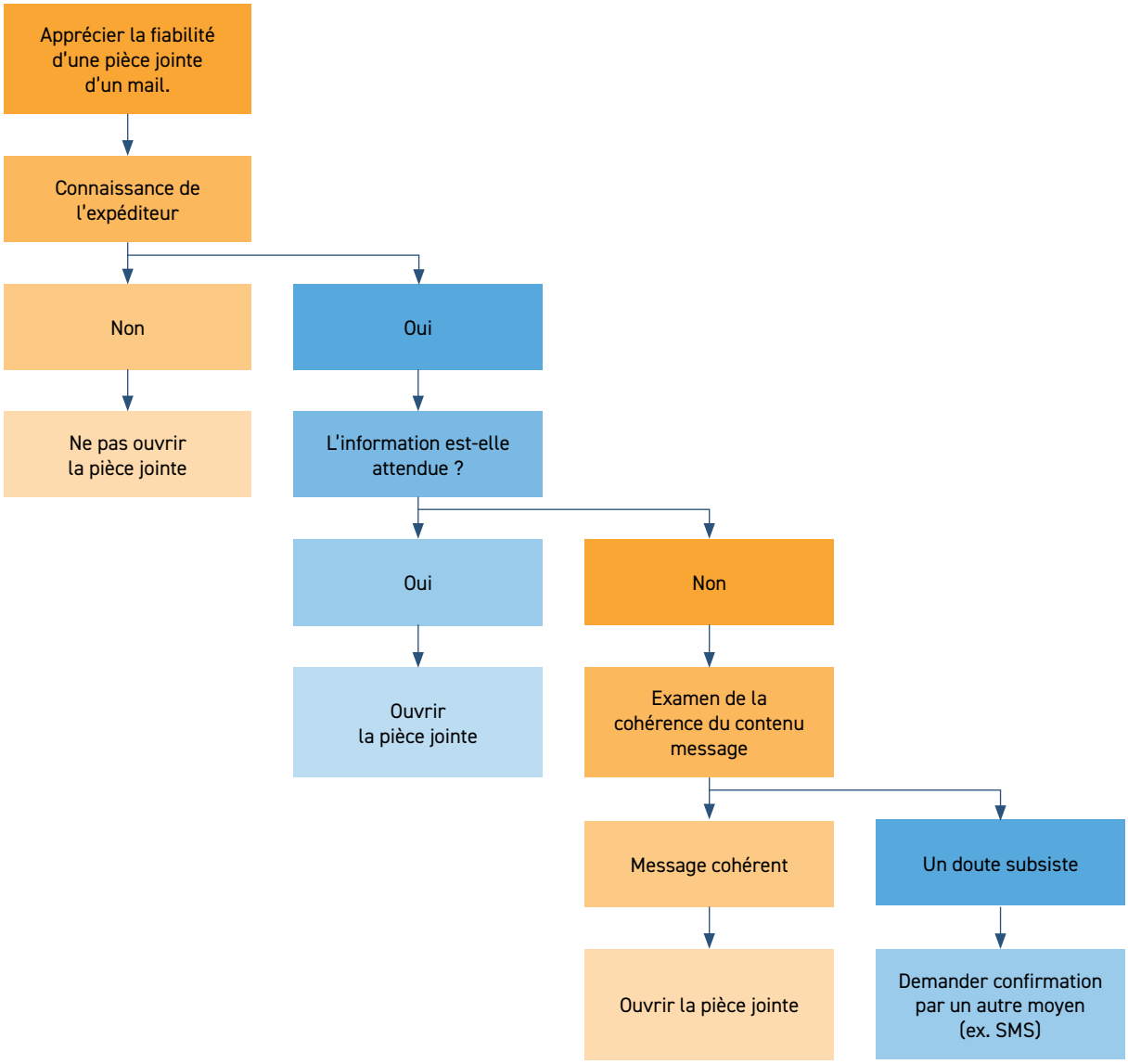
6. Voir en ce sens le rapport de l'ANSSI : Etat de la menace rançongiciel
7. Voir en ce sens le rapport de l'ANSSI : Etat de la menace rançongiciel

- **pour juger de la fiabilité d'une pièce jointe, il convient d'examiner le contexte :**
  - si l'expéditeur est inconnu, il est recommandé de ne pas ouvrir la pièce jointe
  - si l'expéditeur est connu, il convient de vous demander si l'objet est connu ou non c'est-à-dire si l'information est attendue ou non
  - si l'information n'est pas attendue, il est nécessaire de conforter votre analyse par une lecture du corps du message pour s'assurer de sa cohérence
  - si un doute persiste, contactez l'émetteur par une autre moyen (téléphone, SMS) pour obtenir une confirmation

Cette dernière directive est valable dans tous les cas où un mail vous apparaît suspect : il convient alors de contacter l'émetteur du message par un autre moyen (téléphone, SMS si cela est possible).

Il est important d'avoir ces éléments à l'esprit lorsque vous déterminerez la politique de cybersécurité de votre cabinet.

ARBRE DE DÉCISIONS SUR LA FIABILITÉ D'UNE PIÈCE JOINTE



COMMENT SÉCURISER LES EMAILS DU CABINET ?

La sécurisation des emails ne se limite pas à des solutions techniques, mais doit être complétée par des mesures organisationnelles mises en place dans votre cabinet.

La sécurité doit être adaptée à votre cabinet, ce qui implique :

- de choisir la solution de messagerie adaptée (1) ;
- de mettre en place des mesures organisationnelles en mettant en place une politique dans la gestion des emails en fonction de la sensibilité des informations transmises (2).

Quelle solution technique est adaptée au cabinet ?

La question est de déterminer si votre cabinet prend la charge, ou non, de l'infrastructure de messagerie.

Cette question est centrale, car l'infrastructure de messagerie et sa sécurité participent à la protection de votre secret professionnel.

1RE HYPOTHÈSE : votre cabinet ne prend pas en charge l'infrastructure de messagerie – Les offres cloud

Il existe de nombreuses solutions de messagerie sur le cloud, mais très peu remplissent les conditions aptes à garantir une protection du secret professionnel. En effet, les solutions proposées par les sociétés américaines sont soumises à la Foreign Intelligence Surveillance Act qui autorise les administrations américaines à collecter les données personnelles détenues par les personnes morales de droit américain.

C'est la raison pour laquelle le CNB proposera en tout début d'année prochaine une nouvelle solution de messagerie sécurisée avec une adresse structurée en prénom.nom@avocat.fr.

Cette solution fournira aux avocats une solution d'email sécurisée, hébergée en France et respectueuse du secret professionnel.

La connexion à votre boîte email s'effectuera aux moyens de votre clé Avocat ou de votre compte e-Dentitas (authentification double-facteurs). Ceci apportera une sécurisation forte de votre boite email qui n'est, dans les solutions proposées sur le marché, sécurisée que par un mot de passe (l'identifiant étant votre adresse mail que n'importe qui est en mesure de connaître).

Plusieurs offres vous seront proposées à des prix très attractifs.

2E HYPOTHÈSE : votre cabinet prend en charge l'infrastructure de messagerie

Si votre cabinet héberge ou fait héberger son système de messagerie, il doit s'assurer[8] :

☐ **De disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés**

☐ **De l'activation du chiffrement TLS des échanges et en particulier pour les phases d'authentification :**

- entre serveurs de messagerie (de l'entité ou publics)
- entre les postes utilisateurs et les serveurs hébergeant les boîtes de messagerie électronique

Il est par ailleurs recommandé de ne pas exposer directement les serveurs de messagerie électronique sur Internet. Dans ce cas, un serveur relais dédié à l'envoi et à la réception des messages doit être mis en place en cas de coupure d'Internet.

Quelles mesures organisationnelles mettre en place ?

La sécurisation des emails ne dépend pas que de mesures techniques décrites ci-dessus.

Elle doit s'accompagner de mesures organisationnelles, de procédures et process à mettre en place dans vos cabinets dans la gestion de vos emails.

Tous les emails ne requièrent pas le même niveau d'exigence : tout dépend de la sensibilité des informations communiquées. **C'est l'examen de la sensibilité des informations qui détermine le moyen de communication approprié.**

Si les informations ne sont pas sensibles, l'email est le moyen de communication approprié.

Si l'information est sensible c'est-à-dire couverte par le secret professionnel, si elle présente un caractère stratégique pour un dossier, votre cabinet ou si elle est une donnée à caractère personnel, il est recommandé d'éviter de communiquer ce type d'informations dans un email simple.

Quelles est la solution de communication appropriée ?

- **Chiffrer le contenu de votre email** au moyen d'une solution de chiffrement si le contenu de votre email contient des informations sensibles, comme une stratégie dans un dossier
- **Pour l'envoi de pièces à vos clients :** il est recommandé d'utiliser une solution de mise à disposition de documents, plus sécurisée que les emails :
  - le choix de la solution appropriée dépend de la protection du secret professionnel : les solutions proposées sur le marché sont peu nombreuses à garantir une protection du secret professionnel. En particulier, les solutions proposées par les sociétés américaines sont soumises à la Foreign Intelligence Surveillance Act qui autorise les administrations américaines à collecter les données personnelles détenues par les personnes morales de droit américain.

8. Cf. anssi-guide-tpe_pme.pdf

- pour cette raison, le CNB a développé la solution e-Partage sécurisé, respectueuse du secret professionnel de l'avocat et qui vous permet de configurer les conditions de la mise à disposition des fichiers déposés (détermination des destinataires, utilisation d'un mot de passe pour accéder au téléchargement, durée de la mise à disposition, etc.)
  - Pour plus d'informations vous pouvez consulter le guide pratique « Les avocats et le règlement général sur la protection des données, 2e édition, mai 2023 »

- **Pour la réception de pièces de vos clients :** il est recommandé d'ouvrir un lien vers un dossier sécurisé sur une solution de stockage sur le Cloud :
  - Attention au choix de la solution de stockage en ligne appropriée : il est nécessaire que cette solution garantisse le respect de votre secret professionnel. Au risque de nous répéter, les solutions proposées par les sociétés américaines sont soumises à la Foreign Intelligence Surveillance Act qui autorise les administrations américaines à collecter les données personnelles détenues par les personnes morales de droit américain.
  - le CNB proposera en début d'année prochaine une solution de stockage en ligne sécurisée, stockée en France et respectueuse du secret professionnel de l'avocat : vous disposerez de 50Go pour le stockage en ligne.

LA COMMUNICATION DE RIB CARPA

Des cyberattaquants piratent des messageries électroniques avocats et interceptent les emails. Cette interception leur permet ensuite de substituer de fausses coordonnées bancaires (ex : envoyer un faux RIB à la CARPA). La plupart des victimes de fraudes sont des avocats qui ne disposent pas d'une adresse électronique attachée à un nom de domaine professionnel.

Plusieurs bonnes pratiques permettent de prévenir ce risque :

- ne jamais transmettre de RIB par mail et pour les CARPA de ne jamais accepter de RIB transmis par cette voie ;
- de toujours transmettre un RIB via la solution de partage sécurisé du CNB qui est un mode de transmission plus sécurisé que les emails ;
- pour les CARPA, de contacter l'émetteur du message par un autre moyen (téléphone, SMS si cela est possible) pour confirmer le RIB et l'ordre de virement.

Références :

ANSSI, Les mesures cyber préventives prioritaires (2023)

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

ANSSI, Les 10 règles d'or préventives

ANSSI, Panorama de la cybermenace (2022)

FICHE 7
LA SÉCURISATION DU RÉSEAU DU CABINET

CHOISIR ENTRE UN RÉSEAU FILAIRE OU WIFI

Le Wifi est une technologie de transmission d'informations sans fil de la même manière qu'un réseau filaire Ethernet mais sans les mêmes garanties de confidentialité, d'intégrité et de disponibilité.

La technologie Wifi repose sur un lien radio dont les ondes sont par nature sujettes à l'interception et aux interférences (brouillage des ondes accidentel ou intentionnel)[9]. L'enjeu est la protection du système d'information : en effet, un cyberattaquant qui pénètre sur un réseau Wifi peut accéder facilement à d'autres ressources du système (serveurs, équipements réseaux) donc à des données sensibles.

Aussi, **pour les données sensibles, il est recommandé de faire transiter ces données via un réseau filaire Ethernet.**

CONFIGURER UN RÉSEAU WIFI

Si l'utilisation du Wifi est nécessaire à votre cabinet, il est essentiel de sécuriser :

Les points d'accès Wifi

☐ **Utiliser un chiffrement robuste :**

- chiffrement recommandé : WPA2 avec l'algorithme de chiffrement AES-CCMP avec, si nécessaire, une infrastructure d'authentification centralisée
- chiffrement non-recommandé : le WPA-PSK n'est pas recommandé dans le cadre d'un usage professionnel : si vous décidez néanmoins d'y recourir, utilisez un mot de passe long (20 caractères minimum) et complexe que vous changerez régulièrement (tous les 3 mois ou en cas de compromission)

☐ **Ne pas utiliser un SSID (nom de réseau Wifi) trop explicite** sur votre activité professionnelle, n'attirant pas l'attention où ne pouvant pas faire deviner l'activité du cabinet

9. NP_WIFI_NoteTech.pdf (ssi.gouv.fr)

- ☐ **Désactiver le WPS** (Wifi Protected Setup) des points d'accès car il introduit une vulnérabilité importante du point d'accès
- ☐ **Maintenir le microgiciel des points d'accès à jour**
- ☐ **Superviser les évènements de sécurité du point d'accès** (possibilité de mettre en place une supervision centralisée)
- ☐ **Changer les mots de passe par défaut** communiqués par les opérateurs grand public

Définir l'architecture du réseau Wifi

- ☐ **Isoler le réseau Wifi** du réseau filaire en mettant en place des équipements de filtrage réseau
- ☐ **Superviser les évènements de sécurité**
- ☐ **Mettre en place un réseau Wifi « visiteur »** sur une infrastructure dédiée ne donnant accès à aucune ressource du réseau interne
- ☐ **Informer les visiteurs des traitements de données** mis en œuvre dans le cadre d'un réseau Wifi « visiteurs » (RGPD, art. 13)

SÉCURISER LE RÉSEAU DE VOTRE CABINET

Si vous n'avez pas de réseau dans votre cabinet, la première protection indispensable est l'activation du pare-feu intégré dans le système d'exploitation de votre ordinateur (Mac OS, Windows) ou l'installation d'un logiciel pare-feu tierce. Un pare-feu bloque toute connexion entrante.

Si vous avez un réseau informatique au sein de votre cabinet, il est conseillé d'activer ou d'installer un pare-feu sur chaque ordinateur du cabinet.

VOTRE RÉSEAU DOIT RÉPONDRE À CERTAINES EXIGENCES :

☐ **Segmenter le réseau** en mettant en place des zones différentes dans votre réseau et les cloisonner :

- chaque zone a des besoins de sécurité qui doivent être définis (ex. serveurs infrastructure, serveurs métiers, poste de travail utilisateur, poste de travail administrateur, etc.)
- ceci permet de limiter aux cyberattaquants de rebondir sur toutes machines de votre réseau jusqu'à atteindre celles qui contiennent des données sensibles ou critiques

☐ **Mettre en place une passerelle sécurisée d'accès à Internet :**

- au minimum, il est recommandé de mettre en place un pare-feu au plus près de l'accès Internet pour filtrer les connexions et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité afin d'assurer notamment l'authentification des utilisateurs et la journalisation des requêtes
- Enjeu : éviter que des cyberattaquants prennent le contrôle de terminaux à la suite de la consultation d'un site web malveillant ou du téléchargement et l'exécution d'un programme malveillant qui peut bloquer tout le fonctionnement du cabinet, ou exfiltrer des données sensibles ou critiques

☐ **Mettre en place un cloisonnement des services en ligne** offert par votre cabinet, de votre système d'information

☐ **Sécuriser les interconnexions réseau dédiées avec les partenaires** (ex. flux monétique)

☐ **Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques**

Si vous avez besoin de vous faire accompagner pour la mise œuvre de ces mesures, reportez-vous au point 2.10.

Références :

ANSSI, Note technique : recommandations de sécurité relatives au Wifi (2013)

ANSSI, Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux (2018)

ANSSI, Guide d'hygiène informatique pour renforcer la sécurité de son SI en 42 mesures (2017)

ANSSI, La cybersécurité pour les TPE/PME en 13 questions (2022)

FICHE 8
LA MISE EN PLACE D'UN PLAN DE MAINTENANCE DES SYSTÈMES

☐ Mettre à jour les logiciels

Au sein du cabinet, chaque membre utilise quotidiennement différents types de logiciels (navigateur internet, logiciel de gestion du courrier, traitement de texte, visionneuse PDF, application de facturation, etc.) sur ses outils (ordinateurs, téléphones, tablettes, etc.).

Ces logiciels et outils numériques ont accès, et parfois détiennent, certaines données du cabinet.

Aussi, il est important que chaque membre veille **à appliquer les mises à jour de sécurité sur les matériels et les logiciels, dès lors que des correctifs sont proposés par l'éditeur.**

BONNES PRATIQUES

- si le logiciel le permet, il peut être utile pour le membre **d'activer l'option de téléchargement et d'installation automatique des mises à jour des outils et des logiciels les plus courants**. Dans cette situation, il doit tout de même **garder la possibilité d'effectuer des vérifications manuelles** si nécessaire
- si l'un des appareils ou logiciels ne peut plus être mis à jour, le membre concerné doit en informer la personne en charge de la sécurité dans le cabinet afin que celui-ci soit désinstallé et remplacé
- si le cabinet fait appel à des sous-traitants, il est recommandé au cabinet de s'assurer que ces derniers effectuent eux aussi la mise à jour de leurs propres outils et logiciels informatiques et de l'exiger dans les contrats de sous-traitance conclus avec eux.

☐ Mettre à jour le matériel informatique du cabinet

Ce plan doit concerner les serveurs, les ordinateurs du cabinet, le matériel réseau (box internet, routeur, répéteurs, point d'accès, etc.), les imprimantes, les tablettes et smartphones.

FICHE 9
LA SENSIBILISATION ET LA FORMATION DES MEMBRES AU RISQUE NUMÉRIQUE

Afin de s'assurer de l'effectivité des mesures d'hygiène informatique, il appartient au cabinet de sensibiliser et de former les membres au risque numérique qui pèse sur lui ainsi que les enjeux associés à ce risque.

Les chiffres montrent une réelle prise de conscience des dirigeants d'entreprises :

- Le risque cyber est une préoccupation pour plus de 76% des entreprises ;
- 71 % des entreprises de 0 à 9 salariés et 85 % de celles de 10 à 49 salariés sensibilisent leurs collaborateurs aux risques informatiques, dont 44 % tous les ans[10].

Dans les cabinets d'avocats, cette sensibilisation au risque numérique et aux bonnes pratiques de sécurité informatique vise plusieurs types d'utilisateurs : les salariés, les assistants, les collaborateurs (salariés et libéraux), les associés et les prestataires.

S'agissant des risques spécifiques pesant sur le cabinet, il s'agit de permettre aux membres du cabinet de repérer ces risques et de savoir réagir en cas de risque suspecté ou avéré.

L'objectif est de permettre à chaque membre du cabinet concerné de contribuer efficacement à la sécurité informatique du cabinet en faisant prendre conscience :

- des enjeux en matière de sécurité et de vie privée ;
- des risques cyber, qui sont à la fois variés et complexes ;
- des risques spécifiques pesant sur le cabinet (cf. cartographie point n° 1).

10. Voir en ce sens : les 16 chiffres clés sur la cybersécurité des entreprises (- 50 salariés) de la Confédération des PME

Comment sensibiliser/former les membres internes du cabinet (salariés, assistants, collaborateurs, associés) ?

La sensibilisation/formation des membres est essentielle et peut être mise en place en déployant une ou plusieurs des mesures ci-dessous :

☐ Organiser des sessions de sensibilisation et/ou de formation

Il s'agit pour le cabinet de faire prendre conscience aux membres du cabinet des enjeux de sécurité, des mesures préventives à respecter et des bons comportements à adopter.

Il est important de veiller à ce que ces formations/sensibilisations soient régulières, dans un langage clair et adapté au contexte et à l'utilisateur ciblé.

Outre l'organisation de sessions de formation, il est également possible de déployer des actions de sensibilisation par différents canaux : email, affichage dans le cabinet, en réunion, message interne, newsletter, etc.

Il est également possible, si le cabinet dispose d'un espace intranet, de prévoir un espace dédié reprenant toutes les informations transmises lors des sessions et disponible à tout moment pour les membres du cabinet sous forme de fiches pratiques.

Plus concrètement, l'information transmise aux membres du cabinet doit comprendre :

- les objectifs de sécurité fixés et les enjeux que rencontre le cabinet en matière de sécurité informatique

BONNES PRATIQUES

Il peut s'agir aussi lors de ces sessions de formation/sensibilisation d'en profiter pour rappeler des mesures de sécurité plus globale. Exemple : ne pas laisser de document papier confidentiel sur le bureau sans surveillance»

- les informations désignées comme sensibles/confidentielles dans le cabinet et les risques si elles ne sont pas protégées ;
- les règlementations et obligations légales auxquelles le cabinet et/ou les membres sont tenus ;
- les règles de sécurité mises en place dans le cabinet pour traiter les risques ;
- les moyens mis à la disposition des membres pour contribuer à la sécurité de l'information du cabinet ;
- les bons comportements à adopter quotidiennement (ex. verrouiller son poste, mises à jour, etc.) et en cas de risque suspecté ou avéré (ex. procédure à suivre, personne à contacter, etc.) ;
- ou encore, les conséquences potentielles en cas de non-respect des règles de sécurité, etc.

Exemple de formation que l'on peut dispenser aux membres : le cas du « phishing » ou de l'«hameçonnage»

Dans cette situation, il s'agit de former les membres à détecter et à réagir lorsqu'ils reçoivent ce type de messages, en leur indiquant le bon comportement à adopter : ne pas cliquer sur le(s) lien(s), demander aux collaborateurs de faire suivre les emails visés au service dédié (ou à la personne dédiée).

Selon le rapport 2021 de Verizon « Data Breach Investigations Report », 30% des personnes tombent encore dans le piège du phishing par email.

☐ L'organisation d'exercices de mise en situation

Lors des sessions de formation/sensibilisation, il est également possible pour le cabinet d'organiser des exercices de mise en situation ou des tests de sécurité, effectués ou non par des professionnels.

Concrètement, il peut s'agir par exemple d'organiser au sein du cabinet un cas de simulation d'attaque, comme l'envoi de faux messages d'hameçonnage (ou phishing) sur les messageries professionnelles des utilisateurs.

☐ Rédiger une charte informatique

La rédaction d'une charte informatique est également une bonne pratique à adopter pour sensibiliser et responsabiliser les membres sur les mesures préventives du cabinet.

Classiquement, une charte informatique comprend :

- les règles de sécurité de l'information auxquelles les membres doivent se conformer (ex. modalités d'utilisation des moyens informatiques, les règles de sécurité à respecter en cas de vol, la politique de mots de passe du cabinets, les moyens d'authentification, etc.),
- la procédure de déclaration d'un incident à suivre en cas de risque suspecté ou avéré, et,
- les sanctions en cas de non-respect des règles que la Charte énonce.

BONNES PRATIQUES

Afin d'assurer le respect des règles édictées dans la Charte par les membres, il est possible de lui donner force contraignante en l'annexant au règlement intérieur du cabinet.

Quelles bonnes pratiques mettre en place avec les utilisateurs externes (les prestataires et les clients) ?

Pour assurer une sécurité de l'information optimale au sein du cabinet, il est important que chaque utilisateur sans exception soit impliqué.

Dans cette perspective, le cabinet qui doit faire respecter le socle de sécurité de son cabinet aux utilisateurs « externes » peut par exemple prévoir la signature d'un engagement de confidentialité ou d'une clause spécifique dans les contrats de prestation de services.

Références :

ANSSI – Etat de la menace informatique contre les cabinets d'avocats

ANSSI – Guide d'hygiène informatique

Cybermalveillance – Kit de sensibilisation aux risques numériques

FICHE 10
BIEN CHOISIR SES PRESTATAIRES

Il est fréquent que les cabinets de petite taille ou de taille moyenne aient recours à des prestataires informatiques pour sécuriser leur environnement numérique.

Dans le cadre des missions qui leur sont confiées, ces prestataires informatiques ont accès à l'ensemble du parc informatique des cabinets. Une faille dans la sécurité du côté du prestataire peut rejaillir sur le cabinet.

Aussi, il est important que les cabinets s'entourent de prestataires de confiance.

Comment choisir le prestataire et comment avoir confiance ?

Pour répondre à cette question, nous vous proposons une liste de questions que vous pouvez vous poser :

Le prestataire est-il compétent ?

Il est difficile d'évaluer la compétence d'un prestataire qui intervient dans un domaine éloigné de votre expertise avec lequel le cabinet n'a encore jamais travaillé.

Néanmoins, certains éléments peuvent permettre de vous faire une idée :

- qualifications et compétences pour la mission qui lui est confiée ;
- parcours ;
- labellisations ou certifications :
  - le fait que le prestataire soit certifié par le COFRAC à la norme ISO 27001 relative au système de management de la sécurité de l'information
  - le prestataire est labellisé Cyber Expert qui est un label mis en place par Cybermalveillance (cf. Le label ExpertCyber - Assistance aux victimes de cybermalveillance) ;
- niveau de conformité au RGPD et de maturité quant à la protection des données à caractère personnel
  - Nota : les avocats ont l'obligation de ne faire appel qu'à des prestataires qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées en matière de « privacy » ;
- avis sur le prestataire.

La mission confiée au prestataire va-t-elle être exercée par ses soins ou confiée à un sous-traitant ?

Il est important de s'assurer que le prestataire choisi effectue lui-même la prestation qui lui a été confiée. Dans l'hypothèse où la prestation est sous-traitée, il est impératif de s'assurer que le sous-traitant respecte les mêmes exigences que celles qui ont été imposées au prestataire.

Comment sont traitées les informations fournies au prestataire au moment de la mission ?

Les prestataires informatiques ont généralement accès à l'ensemble du parc informatique de leurs clients. Ils bénéficient donc d'importantes informations sur la structure de leur système d'information. Il est nécessaire pour le cabinet de faire signer à son prestataire un accord de confidentialité.

Le prestataire bénéficie-t-il d'une assurance de responsabilité professionnelle ?

En cas d'incident il est possible de se retourner contre le prestataire. Il est important de vérifier qu'il est équipé d'une assurance responsabilité professionnelle susceptible de répondre aux fautes et négligences qui pourraient lui être reprochées.

III. RÉAGIR EN CAS DE CYBERATTAQUE

Le risque numérique zéro n'existant pas, lorsqu'il se réalise et qu'une cyberattaque survient, il est impératif pour le cabinet concerné de réagir rapidement et efficacement afin de traiter et de limiter les impacts de cette crise, de rétablir les services critiques et de maintenir la confiance aussi bien au sein du cabinet que vis-à-vis des clients.

En pratique, cette crise se matérialise par une déstabilisation, voire dans les cas les plus graves par une interruption (totale ou partielle) du fonctionnement courant du cabinet en raison d'une ou plusieurs actions malveillantes, tentées ou commises contre ou grâce aux outils, systèmes et infrastructures informatiques.

Cette déstabilisation force l'organisation à s'adapter et à fonctionner de manière dégradée, et ce, pendant une durée incertaine mais en tout état de cause non négligeable.

Pour pouvoir réagir efficacement, l'organisation doit, au préalable, mettre en place un plan de reprise et de continuité de l'activité informatique. Dans la plupart des cas les cabinets ne disposent pas d'équipe informatique, il peut alors être intéressant de se faire accompagner par un prestataire de service spécialisé.

S'il n'existe pas de modèle type de plan de reprise d'activité, il peut être organisé selon plusieurs axes :

1. Identification des activités qui ne peuvent pas être paralysées
2. Identification des solutions de contournement (ex : retour à la voie papier)
3. Identification des rôles de chaque membre du cabinet en cas d'attaque cyber
4. Procédures à appliquer en cas d'attaque cyber
5. Test du plan de reprise d'activité – Simulation de cyberattaque
6. Mise à jour du plan de reprise d'activité

Ce plan de reprise d'activité se matérialise sous la forme d'un document écrit dans lequel sont présentées les techniques, l'organisation et les actions à mettre en œuvre pour répondre à une cyberattaque.

La détection de l'attaque est le point de départ du traitement de tout incident. Une fois l'attaque détectée et indépendamment du type d'attaque réalisé, il convient de déployer très rapidement certains réflexes :

- [ ] **Déconnecter immédiatement l'ordinateur du réseau en retirant le câble réseau ou en déconnectant le Wifi afin d'éviter la propagation de l'attaque à d'autres appareils**

  (!) POINT D'ATTENTION :

  il ne faut surtout pas éteindre l'ordinateur au risque de perdre les informations utiles sur l'attaque.

  Ne connecter aucun autre appareil sur le réseau

- [ ] **Avertir les membres du cabinet** de la survenance de la cyberattaque
- [ ] **Estimer la situation et ses conséquences prévisibles : si la situation est une crise,** activer une cellule de crise comprenant la totalité des membres du cabinet
- [ ] **Documenter chacune des étapes de l'évènement** en retraçant les faits liés à l'incident (date, heure, contact de la personne ayant découvert l'incident ou ayant été informée de celle-ci, description factuelle) mais également en retraçant, au fur et à mesure, les actions réalisées
- [ ] **Avertir l'assistance technique** (si elle existe) **et/ou la plateforme** cybermalveillance.gouv.fr
- [ ] **Si la situation l'exige, prendre contact avec les autorités** (envisager un dépôt de plainte, déclaration CNIL, etc.)
- [ ] **Communiquer en interne et, si la situation l'exige, en externe** en déployant une communication de crise (notamment avec les médias)
- [ ] **Solliciter, le cas échéant, son assureur** (vérifier votre police d'assurance pour les conditions de déclaration du sinistre et le niveau de prestation auquel vous avez droit)
- [ ] **Restaurer le système d'information depuis de la dernière sauvegarde.**

En principe, cette checklist doit être renseignée par écrit dans le plan de reprise d'activité préalablement construit.

En raison de la diversité des attaques, chaque action déployée devra s'adapter aux spécificités de la crise survenue (nature et ampleur de l'attaque).

En cas d'incident impliquant une violation de données personnelles, il convient aussi pour l'organisation de répondre à ses obligations en matière de protection des données personnelles[11]. Ainsi, à minima, l'incident devra être consigné au sein d'une documentation de violations de données, prenant généralement la forme d'un registre, de l'organisation.

Si la violation est en plus susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, l'organisme devra également procéder à une notification auprès de la CNIL en moins de 72 heures suivant la constatation par le cabinet de l'incident de sécurité.

Lorsque ce risque est élevé, il sera également nécessaire d'informer les personnes concernées en précisant au moins :

- la nature de la violation ;
- les conséquences possibles de la violation ;
- les coordonnées de la personne à contacter (délégué à la protection des données, ou autre référent de l'organisation) ;
- les mesures prises pour remédier à la situation et en limiter les conséquences.

11. Voir en ce sens le service en ligne de la CNIL « notifier une violation de données personnelles » du 24 mai 2018 ainsi que les articles 33 et 34 du RGPD.

RÉFÉRENCES

Cartographie du système d'information, Guide d'élaboration en 5 étapes, ANSSI, 2018

Guide d'hygiène informatique, renforcer la sécurité de son système d'information en 42 mesures, ANSSI, 2017

Générer un mot de passe solide, CNIL

Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité, CNIL

La cybersécurité pour les TPE/PME en 13 questions, ANSSI, 2022

Etat de la menace informatique contre les cabinets d'avocats, ANSSI, 2023

Mesures cyber préventives prioritaires, ANSSI, 2023

Recommandations relatives à l'authentification multifacteur et aux mots de passe, ANSSI

Guide pratique « Les avocats et le règlement général sur la protection des données (RGPD) », 2ème édition, mai 2023

Kit de sensibilisation aux risques numériques, cybermalveillance.gouv.fr

Notifier une violation de données personnelles, CNIL, 2018

Les 16 chiffres clés sur la cybersécurité des entreprises (-50 salariés), CPME, 2019

Note technique, recommandations de sécurité relatives aux réseaux Wi-Fi, ANSSI, 2013

Confiance, qualité, expertise : le label ExpertCyber, Cybermalveillance.gouv.fr, 2021

Etat de la menace rançongiciel à l'encontre des entreprises et des institutions, ANSSI, 2021

Les règles d'or de la sauvegarde, ANSSI

Familles de produits, sauvegarde sécurisée, ANSSI, France Relance

« Cyber-attaques : quels risques sur les sauvegardes et comment s'en protéger ? », RiskInsight, 2021

Rapport cybersécurité, Conseil national des barreaux, AG du 9 décembre 2022

Panorama de la cybermenace 2022, ANSSI, 2023

Anticiper et gérer sa communication de crise cyber, ANSSI, 2021

Organiser un exercice de gestion de crise cyber, ANSSI, 2020

Recommandation de la CNIL sur les mots de passe et autres secrets partagés - Tableau de correspondance avec les recommandations de l'ANSSI, CNIL

Vérifier sa politique de mots de passe, CNIL, 17 octobre 2022

Comment chiffrer ses documents et ses répertoires, CNIL, 2017

Guide de recommandation sur le nomadisme numérique, ANSSI, 2018

Recommandations de déploiement du protocole 802.1 X pour le contrôle d'accès à des réseaux locaux, ANSSI, 2018

Vous pouvez également participer à ces MOOC :

Bienvenue | SecNumacadémie (secnumacademie.gouv.fr)

Le MOOC de la CNIL est de retour dans une nouvelle version enrichie | CNIL

Réglementation en vigueur

- Code des postes et des communications électroniques
- Code du numérique
- Cybersecurity Act, 2019
- Directive Network and Information Security (NIS) : NIS 1 et NIS 2 (entrée en vigueur de NIS 2 prévue en 2024)

Liste des personnes ayant contribué à l'élaboration du guide

Membres de la commission Numérique du Conseil national des barreaux

- Philippe BARON, Président de la commission Numérique
- Clarisse SURIN, Vice-présidente de la commission Numérique
- Olivier COUSIN, Vice-président de la commission Numérique
- Jean BROUIN, Membre de la commission Numérique
- Françoise CASAGRANDE, Membre de la commission Numérique
- Isabelle GRENIER, Membre de la commission Numérique
- Evelyne HANAU, Membre de la commission Numérique

Permanents du Conseil national des barreaux

- Axelle DESHAIRES, Juriste numérique au pôle Ecosystème de la profession, Direction juridique du CNB
- Johan ESPINASSE, Juriste numérique au pôle Ecosystème de la profession, Direction juridique du CNB
- Olivier ZIEGLER, Responsable du pôle Ecosystème de la profession, Direction juridique du CNB
- Thierry BERTE, Responsable de la sécurité des systèmes d'information, Direction générale du CNB
- Guillaume LHUILLIER, Délégué à la protection des données, Direction générale du CNB
- Magguy FERREIRA, Directrice des systèmes d'information du CNB
- Géraldine CAVAILLE, Directrice générale adjointe, Directrice juridique du CNB

CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

1er édition | Octobre 2023
Établissement d'utilité publique
Art. 21-1 de la loi n° 71-1130 du 31 décembre 1971 modifiée

180, boulevard Haussmann - 75008 Paris
Tél. : 01 53 30 85 60 - Fax : 01 53 30 85 62
www.cnb.avocat.fr

Ce document est à destination exclusive des avocats