ASSOCIATION DENTAIRE FRANÇAISE

Commission informatique et numérique

RISQUE CYBER ET ASSURANCES

La cybersécurité d'un cabinet dentaire est cruciale pour protéger la confidentialité des données médicales des patients. Face aux menaces croissantes comme le vol de données et les ransomwares, une protection efficace garantit la sécurité des informations sensibles et la continuité des soins. Pour protéger l'activité du cabinet dentaire, l'ADF met à votre disposition une synthèse simple et pratique des solutions et mesures de protection à observer, réalisée par sa Commission Informatique et numérique.

En quoi consiste ce risque ?

Une cyberattaque sur un cabinet dentaire, souvent provoquée par l'ouverture d'un **e-mail ou le téléchargement d'un fichier frauduleux**, permet aux pirates de prendre le contrôle de vos ordinateurs. Vous perdez alors l'accès à vos services : fichiers, radios numériques, télétransmissions, perturbant ou bloquant ainsi la continuité des soins. Les données des patients, peuvent être revendues sur le dark net. Pour rétablir l'accès une rançon est exigée. Toute cyberattaque affecte aussi la réputation du cabinet et peut entraîner des responsabilités légales, notamment en cas de non-conformité aux normes de protection des données, comme le RGPD.

Quelles solutions ?

Deux volets principaux participent de cette sécurité alors que les risques cyber concernent, à l'heure actuelle, tout type d'activités et, notamment, les activités médicales et la récupération des informations.

- Mesure1 : respecter les protocoles énoncés ci-après.
CECI EST INDISPENSABLE.

- Mesure 2 : souscrire à une assurance contre les risques cyber.
CELA EST FACULTATIF.

Mise à jour le 24 octobre 2024

Mesures de protection cyber importantes à mettre en place au sein de votre cabinet

Utilisation d'un pare-feu	Un pare-feu permet de contrôler les accès au réseau du cabinet médical et de **bloquer les connexions non autorisées**.
Mise à jour régulière des logiciels	Les logiciels utilisés dans le cabinet doivent être régulièrement mis à jour avec les derniers correctifs de sécurité afin de **prévenir les vulnérabilités**.
Utilisation de mots de passe forts	Les mots de passe utilisés pour accéder aux systèmes du cabinet médical doivent être forts et **uniques pour chaque utilisateur.** Il est recommandé d'utiliser des combinaisons de lettres, de chiffres et de caractères spéciaux.
Chiffrement des données sensibles	Les données sensibles, telles que les dossiers médicaux des patients, doivent être chiffrées afin de les **rendre illisibles** en cas de vol ou d'accès non autorisé.
Sensibilisation des employés	Les employés du cabinet doivent être **formés aux bonnes pratiques** de sécurité informatique, notamment en matière de gestion des mots de passe, de détection des e-mails de phishing (non-ouverture) et de protection des données sensibles.
Sauvegarde régulière des données	Il est important de sauvegarder régulièrement les données du cabinet afin de pouvoir les restaurer en cas de perte ou de corruption. **Ces sauvegardes doivent absolument être réalisées à l'extérieur de votre cabinet et susceptibles d'être ré-installées très rapidement après l'attaque de votre système**.
Sauvegarde externe	Lorsque les données sont sauvegardées dans le Cloud, les serveurs doivent respecter les normes spécifiques aux données médicales (cryptage...)
Utilisation d'une solution antivirus et antimalware	Un logiciel antivirus et antimalware doit être installé sur tous les systèmes du cabinet pour **détecter et supprimer** les logiciels malveillants.
Contrôle des accès	L'accès aux systèmes et aux données du cabinet doit être **limité aux personnes autorisées.** Les clés USB ou autres supports ne doivent être utilisés qu'à l'usage exclusif du cabinet. Des mesures telles que la double authentification peuvent être mises en place pour renforcer la sécurité.
Surveillance du réseau informatique	Il est recommandé de mettre en place un système de surveillance du réseau afin de **détecter les activités suspectes et les tentatives d'intrusion.** Des boitiers spécifiques sont proposés par votre maintenance informatique.
Politique de sécurité informatique	Le cabinet doit élaborer et mettre en œuvre une politique de sécurité informatique qui définit **les règles et les procédures à suivre** en matière de protection cyber.

D'autres règles de protection à suivre : Tooth ADF Magazine Cybersécurité.

Les assurances cyber

Nombreux sont les assureurs, mais aussi des banques, à proposer des assurances Cyber.
Voici quelques exemples des garanties offertes :

- Une assurance qui couvre les frais de restauration des données, les pertes d'exploitation, la responsabilité civile professionnelle, la défense pénale, le cyber-chantage, la notification aux patients et aux autorités, et l'assistance juridique et technique.
- Une assurance qui couvre les dommages matériels et immatériels causés par une cyberattaque, les frais de reconstitution des données, la perte de chiffre d'affaires, la responsabilité civile professionnelle, le cyber-extorsion, la notification aux patients et aux autorités, et l'accompagnement juridique et technique.
- Une assurance qui couvre les frais de reconstitution des données, la perte d'exploitation, la responsabilité civile professionnelle, le cyber-chantage, la notification aux patients et aux autorités, et l'assistance juridique et technique.

Les différentes compagnies d'assurance offrent **des garanties complètes et personnalisables selon votre activité et votre niveau de risque**. Pour choisir la meilleure offre pour votre cabinet dentaire, vous pouvez **comparer les tarifs et les conditions** de ces assurances en ligne ou en contactant un courtier spécialisé.
Il faut cependant savoir que ces services n'ont pas été adaptés en première intention à notre activité. Ce sont des déclinaisons au fil des ans de contrats d'assurance pour l'industrie et les grandes entreprises qui ont été les premières a être touchées par des piratages.
Ainsi en général, vous vous rendrez compte que les questionnaires indiquent des items (de CA ou d'activité) nous concernant peu.

Pour bien choisir une assurance et un montant de prime afférant, dans la mesure ou une attaque cyber, contrairement à d'autres activités, nous pénalise énormément mais ne nous empêche pas totalement de travailler (les actes en bouche sont toujours réalisables) la négociation doit tenir compte de ces éléments afin de mettre en adéquation la prime et le risque.

En conclusion, ce qu'il faut retenir

- Il faut **être à jour de ses maintenances de logiciel** ; surtout en ce qui concerne les sauvegardes.
- Les **services informatiques** qui assurent la maintenance de votre installation **doivent être sécurisés** par le biais de boitiers spécifiques.
- Vous devez **respecter toutes les consignes de sécurisation** liées à votre exercice. Ce sera d'ailleurs la condition de prise en charge par une assurance.
- Vous devez **souscrire une assurance** afin de couvrir les frais éventuels liés à un piratage et notamment les obligations du RGPD.

Voici des exemples de propositions qui sont faites à notre profession. Comme vous le constaterez, elles ne sont pas spécifiques à notre activité mais elles peuvent nous orienter quant aux choix à faire.

Qu'est-ce qui est assuré ?

Les garanties sont limitées à des plafonds qui varient en fonction du montant choisi. Une somme peut rester à la charge de l'assuré.

LES GARANTIES SYSTÉMATIQUEMENT PRÉVUES

1. Assistance (sans franchise pour les entreprises dont le chiffre d'affaires est inférieur à 25 millions €)
    - Expert en sécurité
    - Avocat
    - Expert en communication de crise
    - Expert en récupération de données.
2. Dommages subis par l'assuré
    - Violation de données personnelles : frais de notification, centre d'appel…
    - Atteinte aux données confidentielles
    - Perte d'exploitation.
    - Frais supplémentaires d'exploitation.
3. Dommages causés aux tiers
    - Atteinte à la sécurité et/ou à la confidentialité des données personnelles : frais de défense, dommages et intérêts, mesures correctives.
    - Cyber-responsabilité : frais de défense, dommages et intérêts, mesures correctives.
    - Atteinte aux données confidentielles de tiers : frais de défense, dommages et intérêts, mesures correctives.
    - Virus et attaque par déni de service : frais de défense, dommages et intérêts, mesures correctives.
4. Enquêtes et sanctions
    - Frais de défense
    - Amendes et pénalités légalement assurables.
5. Cyber-extorsion.

LES GARANTIES OPTIONNELLES

- Cyberfraude (plafond maximum de 250.000 €)
- Piratage de ligne téléphonique (plafond maximum de 250.000 €)
- Interruption des activités professionnelles – défaillance de fournisseurs de services informatiques et/ou externalisés (sur demande)
- Interruption des activités professionnelles – défaillance du système informatique de l'assuré (sur demande)
- Fraude élargie à l'ingénierie sociale (sur demande).

Où suis-je couvert(e) ?

La couverture est valable dans le monde entier à l'exclusion des litiges devant les juridictions des Etats-Unis et du Canada (ou relevant du droit de ces pays) pour l'ensemble de garanties.

Qu'est-ce qui n'est pas assuré ?

Les risques lies à une activité dans les domaines suivants : institutions financières, services financiers, courtage, assurances, compagnies aériennes, gouvernements, agences de notation, réseaux sociaux, nucléaire, aéronautique, aérospatial, fournisseurs d'utilités, paris et jeux d'argent, parcs d'attraction, détectives et enquêteurs privés, portails et processeurs de paiements, éditions ou exploitation de logiciels de contrôle de process industriel, industries extractives, diagnostic immobilier, activités contraires aux bonnes mœurs.

Y a-t-il des exclusions à la couverture ?

PRINCIPALES EXCLUSIONS

- Les dommages matériels et corporels.
- Les sinistres liés à la guerre civile ou étrangère, et aux désordres civils.
- Les frais de reconstitution des données en l'absence de procédure, de sauvegarde mensuelle au minimum.
- Les sinistres résultants de toute atteinte à des brevets.
- Les sinistres causés par tout évènement naturel.
- Les sinistres causés par tout tiers fournisseur d'utilités.
- Les sinistres résultant de tout manquement aux obligations contractuelles de l'assuré, sauf lorsque sa responsabilité aurait été engagée dans les mêmes termes en l'absence de contrat.
- Les sinistres résultant de toute violation par l'assuré de toute règlementation boursière, financière ou comptable et/ou fiscale.
- Les amendes, impositions, taxes, pénalités et/ou toutes autres sanctions pécuniaires, (sauf pour la garantie « Enquêtes et sanctions » dès lors que les sommes sont légalement assurables).
- Le paiement direct d'une rançon préalablement à toute déclaration de sinistre par l'assuré.
- Les sinistres résultants de sols, pertes et détournements (sauf pour la garantie « fraude et surfacturation »).
- Les sinistres résultant de la collecte et traitement illégal(e) de données personnelles / spamming.

PRINCIPALES RESTRICTIONS

- Une somme peut rester à la charge de l'assuré (franchise).
- Les garanties ne sont pas mobilisables en cas de passé connu, faute intentionnelle ou fausse déclaration du risque.
- L'accord préalable de l'assureur est nécessaire pour permettre la prise en charge des frais de défense, des frais additionnels et des conséquences d'un accord amiable avec le tiers réclamant.
- Les garanties ne sont pas dues lorsqu'il est avéré qu'elles sont contraires à une sanction économique prévue par les Nations-Unies, l'Union Européenne ou tout autre État.