kaspersky

PROTECTION DES DONNÉES DE SANTÉ : DU CURATIF AU PRÉVENTIF

MANIFESTO
2019

LA DONNÉE DE SANTÉ
A UN PRIX

350 euros. C'est le prix de vente d'un dossier médical sur le marché noir numérique, soit 2,5 fois plus que la moyenne mondiale des autres documents. Et pour cause, ils sont de véritables mines d'or pour les cybercriminels. Ils concentrent énormément d'informations à caractère personnel extrêmement sensibles telles que nos dates de naissance, adresses postales, numéros de sécurité sociale et de mutuelle, données biométriques ou encore coordonnées bancaires[1].

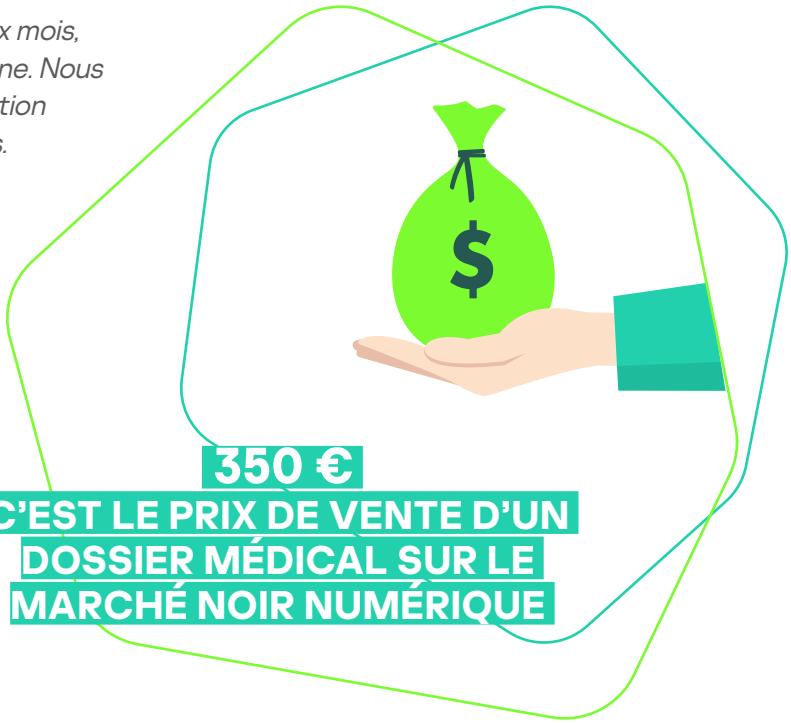
Du fait de leur sensibilité, les données médicales sont une cible de choix pour les cybercriminels et, par ricochets, les entreprises et établissements de santé subissent depuis plusieurs années des salves continues d'attaques. Entre 2017 et 2018, les attaques informatiques visant des données médicales ont été multipliées par trois[2] et le rythme semble plus que jamais s'accélérer.

Le danger s'est accru depuis le début de l'année [2019]. Les alertes sérieuses, qui survenaient habituellement tous les mois ou tous les deux mois, suivent désormais le rythme d'une par semaine. Nous sommes obligés de réagir, il s'agit d'une question d'éthique lorsque des hôpitaux sont touchés.

Guillaume Poupard,
Directeur général de l'ANSSI[3]

Le numérique est partout et parfois là où on ne l'attend pas. Il n'est pas toujours évident de prendre en compte l'ampleur de l'infrastructure à protéger. Les organisations de santé utilisent chacune de très nombreux équipements reliés entre eux et connectés à Internet : matériel biomédical, ordinateurs professionnels, appareils mobiles… À cela s'ajoutent le nombre et la grande diversité des acteurs impliqués dans la production de la donnée de santé ou son cycle de vie, depuis les praticiens jusqu'aux patients, en passant par les experts technologiques. Tous ne sont pas des spécialistes en cybersécurité et c'est bien normal. Mais ils restent vulnérables aux mêmes types d'attaques que les autres secteurs et doivent en être conscients, d'autant que la sécurité des patients dépend de celle de leurs données médicales.

Tanguy de Coatpont,
Directeur général de Kaspersky France



1 Ponemon Institute : 2017 Cost of a Data Breach Study Global Overview
2 Protenus 2019 Barometer
3 Les hôpitaux français dans le collimateur des pirates informatiques, l'Express, 25 juin 2019

L'ENJEU
DE SENSIBILISATION

Les gouvernements du monde entier commencent à prendre la mesure des menaces qui pèsent sur les établissements de santé. En France, le Ministère des Solidarités et de la Santé a annoncé en avril 2019 la stratégie « Ma santé 2022 ».

Ce dernier inclut un vaste chantier numérique visant à transformer le système de santé actuel pour gagner en efficacité et en qualité. Tous les acteurs du secteur, publics comme privés, pourront participer à l'élaboration de la nouvelle infrastructure de santé à condition qu'ils soient en conformité avec les règles et principes édictés. Pour les professionnels de santé, les premiers responsables de la protection des données des patients sont :
les établissements de santé (32 %), l'Etat et les instances gouvernementales (30 %), les praticiens eux-mêmes (15 %), les patients (6 %), ne savent pas (16 %).

Tous seront moteurs à leur niveau, qu'il s'agisse de médecins, patients, fournisseurs technologiques privés, du gouvernement... Le changement est avant tout culturel et non pas technologique ; il faut amener la profession à voir l'intérêt du numérique et de la sécurité des données, leur en présenter les bénéfices pour le système dans son ensemble et pour chacun d'entre eux. Le changement doit être désiré par le plus grand nombre pour rencontrer le moins d'opposition possible.

Gilles Castéran,
Directeur exécutif d'Accenture Sécurité France

Amenés à manipuler quotidiennement les données patients, les professionnels de santé sont 70 % à se déclarer concernés par les questions de cybersécurité et de protection de la vie privée. Ce pourcentage est extrêmement encourageant et confirme le succès des campagnes de sensibilisation nationales menées auprès de cette population. Les efforts doivent continuer pour mobiliser les 30 % qui répondent par la négative ou avouent ne s'être jamais posé la question.
Interrogés sur les mesures de sécurité mises en place pour protéger les données de santé, 24 % avouent leur dénuement en répondant « je ne sais pas ».

Je suis convaincu que l'un des freins à la pleine adoption du numérique dans le secteur de la santé reste la défiance qu'il inspire. La cybersécurité est l'un des éléments qui permettra d'établir cette confiance nécessaire, au même titre que la transparence et le respect des règles.
En France, le changement est long à s'imposer mais une fois le processus enclenché, la mise en action peut être très rapide. Les bénéfices apportés par le numérique sont tels, pour les professionnels comme pour les patients, que nous devrions surmonter ces obstacles rapidement.

Tanguy de Coatpont,
Directeur général de Kaspersky France

55% des professionnels de santé estiment ne pas disposer des ressources et moyens nécessaires pour garantir efficacement la sécurité et la confidentialité des données numériques des patients. Parmi les raisons évoquées : **32 % considèrent manquer de connaissances et de formation sur le sujet. Seuls 11 % ont été formés aux enjeux de cybersécurité au cours des 24 derniers mois,** alors même que le RGPD est entré en application il y a un peu plus de 17 mois, **17 % estiment manquer de ressources financières, 14 % pensent qu'il est difficile de concilier la protection des données et les contraintes professionnelles liées à l'usage de ces données, 13 % avouent manquer de temps.**

Il est de coutume de dire que le maillon faible est l'utilisateur mais avec une sensibilisation constante au sujet de la cybersécurité, il pourrait devenir le maillon fort. On observe une véritable volonté de l'ensemble des acteurs du domaine médical d'avancer dans ce sens. Nous sommes dans une démarche d'humanisme numérique au service de l'usager et de sa santé ; cela passe par un engagement collectif. En matière de cybersécurité, les établissements de santé sont de plus en plus sensibilisés mais il reste encore une marge de progression ; il y a un écart énorme entre connaissance et capacité à traiter un sujet avec une mise en place exponentielle des dispositifs numériques.

Philippe Loudenot,
Fonctionnaire à la sécurité des systèmes d'information (FSSI), Ministère des Solidarités et de la Santé

LES ATTAQUES
VECTEUR DE SENSIBILISATION À RETARDEMENT

Si les professionnels de santé sont relativement peu protégés face aux cyberattaques, ils sont paradoxalement 59 % à considérer la dématérialisation des données de santé comme un risque pour la confidentialité des échanges. De plus, 62 % craignent de voir ces données dématérialisées exploitées à des fins autres que médicales. Preuve de l'urgence à protéger les données de santé et former ceux qui les manipulent, 10 % des sondés admettent avoir été victimes d'une fuite de données ou d'une attaque au cours des derniers mois.

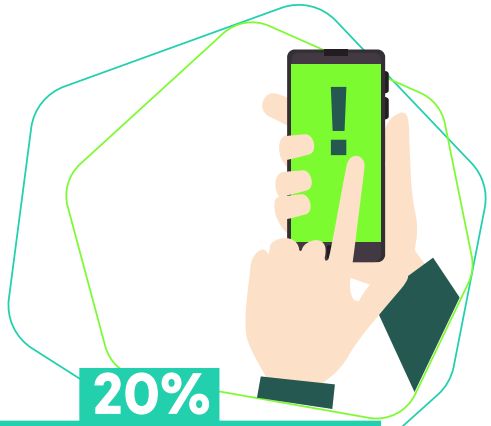
Les incidents informatiques ont une véritable influence sur la mise en place de procédures de sécurité. Parmi les répondants ayant été victimes d'une attaque : **35 % ont installé une solution de sécurité sur tous les appareils qu'ils utilisent dans le cadre professionnel (contre 18 % des sondés n'ayant pas été touchés par un incident de sécurité), 28 % ont installé une solution de sécurité sur une partie de ces appareils (contre 6 % des sondés n'ayant pas été touchés par un incident de sécurité), 17 % utilisent des méthodes de chiffrements (contre 4 % des sondés n'ayant pas été touchés par un incident de sécurité).**

L'adoption des bonnes pratiques reste très faible au regard des efforts de sensibilisation réalisés et de la criticité des données de santé. La cybersécurité, et l'informatique en général, ne sont en effet pas la raison d'être des établissements de santé qui allouent une large partie de leurs ressources aux soins. Les DSI peuvent donc rencontrer des difficultés à conserver les infrastructures informatiques à niveau et même parfois à recruter des experts compétents.

Tanguy de Coatpont,
Directeur général de Kaspersky France

On observe une accélération des efforts de sensibilisation lorsque de grands incidents de cybersécurité font la une de l'actualité. L'émotion conduit la population à y prêter plus d'attention pendant un temps, mais les mauvaises habitudes reprennent vite le dessus. On observe des comportements similaires lors d'un incident routier ; les automobilistes ralentissent pendant quelques kilomètres par précaution puis reviennent à leur vitesse initiale. L'un des principaux enjeux est de maintenir durablement cette attention. Les RSSI doivent pouvoir présenter le risque au sein d'une logique complète, c'est-à-dire en indiquant qu'elles peuvent être les conséquences. La cybersécurité ne doit pas être une fin en soi mais un outil au service de métiers et des personnes. C'est l'impact sur le patient ou sur la capacité d'un médecin à faire son travail qui importe.

Philippe Loudenot,
Fonctionnaire à la sécurité des systèmes d'information (FSSI), Ministère des Solidarités et de la Santé



20%
SEULEMENT ONT RECOURS À UNE SOLUTION DE SÉCURITÉ SUR TOUS LES APPAREILS QU'ILS UTILISENT

UNE (TROP) LARGE VARIÉTÉ D'APPAREILS

Les établissements de santé ne sont pas tous égaux en matière de maturité numérique.

Historiquement, l'essor de l'informatique dans les établissements de santé a conduit les praticiens à imposer leurs habitudes et appareils numériques personnels à leur Direction des Services d'Information. La pratique du « bring your own device » (BYOD) était même parfois plébiscitée par les responsables eux-mêmes car moins coûteuse que la mise à jour du parc complet des équipements.

Tanguy de Coatpont,
Directeur général de Kaspersky France

Les professionnels de santé utilisent majoritairement leurs appareils personnels pour créer, modifier ou partager des données de santé : **smartphone personnel (42 %), ordinateur portable personnel (29 %), tablette personnelle (17 %), smartphone professionnel (4 %), ordinateur portable professionnel (7 %), ordinateur de bureau professionnel (8 %), tablette professionnelle (3 %).**

Lorsqu'un secteur entame sa transformation numérique, l'usage s'impose avant d'être règlementé par les politiques de sécurité et non l'inverse. Les gens utilisent donc leurs propres appareils et services. C'est particulièrement vrai dans l'écosystème médical, qui est pensé pour être au service des médecins. D'autre part, il faut garder à l'esprit que nous ne sommes pas égaux face au numérique ; l'impact de la fracture générationnelle ne s'arrête pas aux portes des entreprises . Le métier aura mis longtemps à adopter le numérique mais son intégration est maintenant très rapide et crée beaucoup de valeur. Les mentalités changent.

Gilles Castéran,
Directeur exécutif d'Accenture Sécurité France

Problème : si 58 % des sondés s'estiment matures - eux-mêmes ou leur établissement - en matière de sécurité informatique, près d'un quart des professionnels de santé interrogés (22 %) n'ont aucune solution de sécurité en place, alors même que les menaces mobiles sont les menaces qui croient le plus vite. Les chercheurs de Kaspersky ont vu le nombre d'attaques de malware sur mobiles pratiquement doubler entre 2018 et 2019[4].

Pour protéger leurs appareils et garantir la confidentialité des données qui y sont conservées : **20 % des professionnels de santé ont recours à une solution de sécurité sur tous les appareils qu'ils utilisent dans le cadre professionnel, 8 % des professionnels de santé ont recours à une solution de sécurité sur une partie seulement des appareils utilisés dans le cadre de leur activité. Seuls 7 % des sondés revendiquent l'utilisation d'une solution de chiffrage des e-mails ou d'une messagerie chiffrée. Seuls 5 % des sondés chiffrent les données stockées sur leurs équipements.**

Il nous faut compléter le mode réactif actuel avec un mode préventif en proposant des solutions de cybersurveillance adaptées et en rappelant les fondamentaux. Cela implique d'avoir un anti-malware à jour, faire des sauvegardes offline des dossiers, ne pas surfer sur Internet avec du matériel obsolète, avec des comptes à privilèges ou cliquer sur des liens d'origine inconnue... Malheureusement, les incidents de sécurité sont bien souvent la conséquence d'un manque de suivi de ces bonnes pratiques, même s'il faut aussi reconnaître que les attaques sont de mieux en mieux élaborées .

Philippe Loudenot,
Fonctionnaire à la sécurité des systèmes d'information (FSSI), Ministère des Solidarités et de la Santé

4 Mobile : Le nombre d'attaques de malware a doublé en 2018, Kaspersky, 13 mars 2019

SÉCURISER LES ÉCHANGES D'INFORMATIONS

Outre le gain de temps réalisé sur les tâches administratives constaté par 57 % des sondés, la dématérialisation des données de santé permet également pour la moitié des interrogés (50 %) de communiquer plus facilement avec leurs patients. On observe une large dominance des outils de communication grand public, au détriment des outils professionnels, en raison de la nécessité pour le médecin et son patient de disposer du même moyen de communication.

En France, il existe beaucoup d'outils à destination des médecins et l'offre est donc très morcelée. Chacun utilise donc l'outil qu'il veut ou celui dont il dispose ; l'ensemble manque parfois de cohérence et d'interopérabilité. Heureusement le marché devient de plus en plus mature et l'hétérogénéité est en passe de se résoudre.

Gilles Castéran,
Directeur exécutif d'Accenture Sécurité France

Parmi les outils numériques utilisés par les professionnels de santé pour communiquer avec leurs patients ou partager avec eux des informations personnelles, on retrouve : **les e-mails (33 %), les SMS (27 %), WhatsApp (11 %), les applications professionnelles (7 %), Skype (6 %), FaceTime (4 %).**

Pour les médecins, la confidentialité des échanges est une règle sacrée. Afin de conserver ce lien de confiance entre patients et professionnels à l'ère numérique, il est impératif que la donnée soit protégée. Les nouvelles technologies peuvent changer le rôle de certains acteurs et il faut les accompagner pour lever leurs craintes et montrer que cela est une évolution positive. Cela passera par la construction d'une vision globale de l'apport du numérique dans la santé et par l'instauration de points d'étapes réguliers pour dynamiser cette évolution.

Tanguy de Coatpont,
Directeur général de Kaspersky France

Le chiffrement de WhatsApp est présenté comme étant un chiffrement de bout en bout, ce qui signifie que les messages sont chiffrés sur le terminal de l'expéditeur et déchiffrés sur celui du récepteur, sans qu'aucun intermédiaire ne soit en mesure de déchiffrer ceux-ci. En revanche, la confidentialité et la sécurité des informations ne sont que partielles si le téléphone lui-même n'est pas protégé et donc accessible facilement à un tiers.

Les professionnels de santé disposent pourtant d'outils spécifiques tels qu'une messagerie sécurisée mise à disposition par les pouvoirs publics et d'autres via des opérateurs privés. Il est dommage de constater que certains médecins utilisent des méthodes grand public qui ne sont pas spécifiquement sécurisées, car tous les échanges relatifs aux données de santé doivent se faire de façon sécurisée. Et si une information médicale doit être transmise à un non-professionnel, comme les patients ou les accompagnants qui concourent aux rapports de soin, il faut utiliser des méthodes de chiffrement.

Philippe Loudenot,
Fonctionnaire à la sécurité des systèmes d'information (FSSI), Ministère des Solidarités et de la Santé

CONCLUSION
LES RECOMMANDATIONS DE KASPERSKY

L'arrivée du numérique dans le domaine médical oblige les acteurs de ce secteur ainsi que les patients à revoir leur rapport aux risques. Le BYOD, la numérisation des informations des patients sur une très large variété de supports mais également la dématérialisation des échanges avec le personnel médical et l'utilisation accrue d'objets connectés sont autant d'usages qui requièrent aujourd'hui une sensibilisation continue aux questions de sécurité informatique. Le virage numérique pris par le secteur de la santé est source d'opportunités pour tous les acteurs de la chaîne. Si nous souhaitons faire en sorte qu'il le reste, ce virage doit être contrôlé et raisonné.

Pour Kaspersky, l'urgence repose sur l'adoption de 3 bonnes pratiques simples à mettre en place dans tous les établissements.

1 **Sensibiliser tous les acteurs impliqués à la cybersécurité.** Il est primordial d'avoir une vision à long terme et de proposer des outils et programmes permettant non seulement la formation régulière et récurrente, mais aussi le contrôle des connaissances et leur mise en application. Il est indispensable que chaque acteur, au niveau individuel et quelles que soient ses responsabilités, ait le réflexe de n'utiliser que des appareils et logiciels sûrs, mis à niveau systématiquement. On ne saurait trop rappeler que le meilleur moyen de se protéger des cybercriminels est de limiter la création de failles et vulnérabilités.

2 **Savoir identifier les besoins et s'entourer d'experts.** La sécurité informatique ne doit pas se résumer à l'achat d'une solution de sécurité ; ce n'est que l'une des nombreuses étapes de toute stratégie transformationnelle. Chaque structure a des besoins spécifiques en fonction de sa taille, ses outils et son fonctionnement. C'est particulièrement vrai dans le secteur de la santé, qui regroupe aussi bien des praticiens de ville isolés que des grands groupes hospitaliers et qui connaît d'importantes disparités budgétaires d'un acteur à l'autre.

Instaurer une stratégie de sécurité adaptée commence pas la réalisation d'une cartographie du réseau et des équipements qui le composent, afin d'identifier les failles potentielles et les axes d'améliorations. Cela permet d'optimiser l'efficacité des dispositifs de protection et de limiter les dépenses inutiles. L'étape suivante consiste à s'entourer de spécialistes capables d'intégrer la sécurité informatique dans une approche globale. Le paysage des menaces évolue rapidement et peu d'entreprises disposent aujourd'hui des compétences internes suffisantes pour suivre le rythme. S'appuyer sur un réseau d'experts permet de rester à la pointe, face à des cybercriminels toujours plus inventifs.

3 **Réorganiser les infrastructures du système de santé et les structures affiliées (médecins libéraux, cliniques et hôpitaux privés comme publics, Assurance Maladie, mutuelles, opérateurs privés…).** La mise en place de tels outils et de stratégies de cybersécurité efficaces nécessite la collaboration de l'ensemble des institutions et celle de nombreuses fonctions professionnelles, de la DSI aux RH en passant par les comités d'administration. L'objectif est d'intensifier l'interopérabilité des systèmes d'information en santé, ce qui conduira à les rendre plus sûrs.

Conscient de ces enjeux, le gouvernement a d'ores et déjà impulsé des changements et annoncé une feuille de route ambitieuse. Le 25 avril 2019, Agnès Buzyn, ministre des Solidarités et de la Santé, et Cédric O, secrétaire d'État chargé du numérique, ont présenté leur programme en matière de numérique en santé, défini dans le cadre de la stratégie de transformation du système de santé : Ma Santé 2022. En filigrane, le futur numérique du secteur de la santé se construit autour de 3 maîtres mots : sécurité, interopérabilité et complémentarité.

Dans la course à l'évolution numérique, la protection des données de santé se présente comme un relais. L'administration et la sécurisation de ces données sensibles éparses ne doivent être qu'un obstacle périodique à dominer, et non un état de fait dont l'on doit se satisfaire.

Kaspersky France remercie chaleureusement pour leur participation
Gilles Castéran, Directeur exécutif d'Accenture Sécurité France
Philippe Loudenot, fonctionnaire à la sécurité des systèmes d'information (FSSI), Ministère des Solidarités et de la Santé

Méthodologie de l'étude

Cette étude a été menée par Yougov pour Kaspersky France en juillet 2019, auprès d'un panel de 1 002 professionnels de santé en France. Les participants ont été interrogés en ligne sur leur perception de la sécurité informatique et l'état des lieux de cette dernière dans leur quotidien. Les données sont pondérées pour être représentatives de la population des professionnels de santé.

À PROPOS DE KASPERSKY

Kaspersky est une société de cybersécurité mondiale fondée en 1997. L'expertise de Kaspersky en matière de « Threat Intelligence » et sécurité informatique vient perpétuellement enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky aident plus de 400 millions d'utilisateurs et 270 000 entreprises à protéger ce qui compte le plus pour eux. Pour en savoir plus : www.kaspersky.fr.

Pour plus d'informations sur l'actualité virale : **www.securelist.com**
Blog français de Kaspersky : **http://blog.kaspersky.fr**

CONTACTS PRESSE
OPRG pour Kaspersky

Alexandra Kohl – 01 53 32 57 73
Marianne Negrello – 01 53 32 55 99
Jules Triolaire – 01 53 32 56 50
Alexandre Ménard – 01 53 32 55 35
Marion Delmas – 01 53 32 55 61

france.kaspersky@omnicomprgroup.com