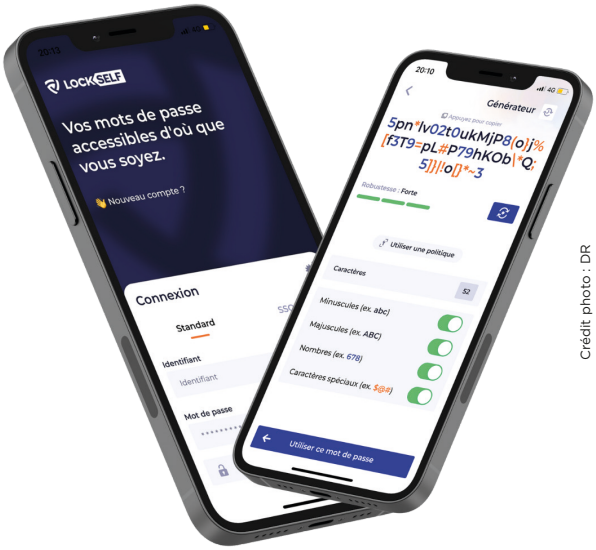
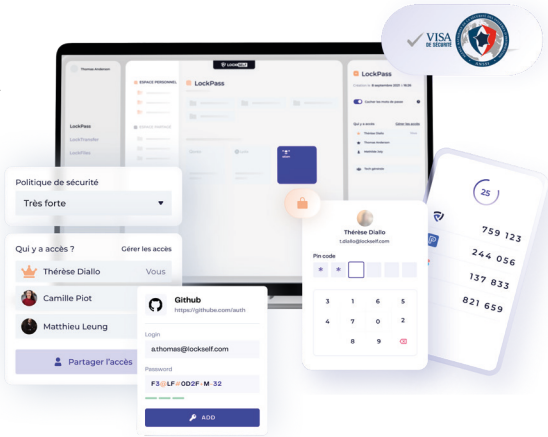
LE CHU DE LA MARTINIQUE RENFORCE LA SÉCURITÉ DES ÉCHANGES ET DES MOTS DE PASSE

De plus en plus ciblés par des cyber-attaques, les établissements de santé cherchent les parades à ces menaces. L'éditeur Lockself réponds à cette préoccupation, avec une suite d'outils logiciels dédiés à la sécurité : gestionnaire de mots de passe, système de stockage et chiffrage des données sensibles mais aussi modules de messagerie sécurisée. Ces solutions sont certifiées CSPN par l'ANSSI (*). « *Nous répondons à des besoins très spécifiques des établissements hospitaliers, explique Pierre Rangdet, directeur des opérations chez Lockself. Nous venons remplacer Keepass au sein des DSI et aidons à la suppression des mauvaises pratiques pour les directions 'support'. Sur la partie partage sécurisé de fichiers, nos outils sont complémentaires des messageries sécurisées de santé afin de limiter le shadow IT et de permettre aux agents qui ne sont pas professionnels de santé de partager des documents de manière sécurisée.* »



Crédit photo : DR



Crédit photo : DR

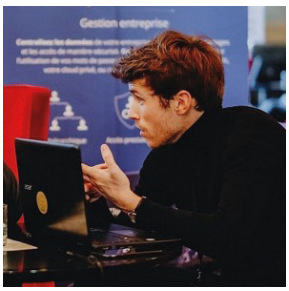
Pour les mots de passe, ils sont exportés dans l'outil maison, et donc protégés. Il est aussi possible d'instaurer une gestion partagée de ces mots de passe, grâce à une arborescence qui donne accès, de façon très intuitive, aux personnels ou aux groupes que l'on choisit, tout en assurant une bonne traçabilité. L'administrateur peut ainsi réaliser des audits de comptes, ou recevoir des notifications en cas de problème. De quoi réduire très fortement la « surface d'exposition » aux attaques, notamment de type ramsonware. Le logiciel est hébergé, au choix, en interne, sur un cloud public ou sur un cloud privé (Outscale, de Dassault Systèmes).

Un autre outil de Lockself permet de chiffrer l'envoi des e-mails, grâce à l'ajout d'un plug-in sur la messagerie. On peut ainsi sécuriser les échanges – notamment entre les professionnels de santé et ceux d'autres métiers – sans changer les habitudes de travail. Enfin, un « coffre-fort numérique » permet de protéger les données sensibles et de les partager simplement entre les différents établissements d'un GHT par exemple.

L'EXEMPLE DU CHU DE MARTINIQUE

Engagé dans un vaste chantier de transformation numérique, le CHU de Martinique a adopté deux solutions Lockself : le gestionnaire de mots de passe et le système d'échange sécurisé de documents. Ils s'ajoutent à une série de mesures mises en place depuis quelques mois pour renforcer la sécurité : audits sur la vulnérabilité aux cyber-attaques, adoption de process de fonctionnement en mode dégradé ou en cas de découverte d'une faille de vulnérabilité, instauration d'une procédure d'identification multifacteurs pour les collaborateurs... « *La sécurité est l'affaire de tous, rappelle Gérald Galim, responsable de la sécurité du système d'information (RSSI) au CHU. Chacun doit être attentif. A nous de sensibiliser les personnels et de leur inculquer les bons réflexes – par exemple pour la gestion des mots de passe. Les solutions Lockself nous y aident.* »

LOCKSELF



Pierre Rangdet
Directeur des opérations chez Lockself
Crédit photo : DR

Gérald Galim
Responsable de la sécurité du système d'information (RSSI) au CHU
Crédit photo : DR

« *En matière de cyber-sécurité, nous étions jusqu'à une date récente en situation de maturité imparfaite*, observe de son côté Rodrigue Alexander, directeur au CHU martiniquais depuis avril 2022, en charge du numérique, du biomédical, de la qualité, de la recherche et des relations avec les usagers. *Malgré nos progrès, nous ne sommes pas encore au niveau requis, car la menace s'intensifie. Nous devons redoubler d'efforts.* »

Aujourd'hui, Lockself équipe une cinquantaine de structures hospitalières (et notamment des GHT), en métropole et aux Antilles. L'éditeur prévoit de proposer très bientôt une plateforme intégrée de gestion sécurisée de documents entre différents établissements. « *De façon générale, nos solutions permettent de gérer de manière simple et fluide, depuis un endroit unique, l'ensemble des tâches liées à la sécurisation des données* », souligne Pierre Rangdet.

J.-C. L.

(1) Certification de premier niveau, délivrée par l'Anssi (Agence nationale de la sécurité des systèmes d'information).

POUR EN SAVOIR PLUS :