INNOVATION & SOLUTIONS | CYBERSÉCURITÉ | NEWS
Publié le 01 novembre 2021, 08:59. Modifié le 01 novembre 2021, 13:27.

Victime d'une cyberattaque, l'EMS Maison de Vessy témoigne

par Grégoire Barbey

L'EMS Maison de Vessy est l'un des trois plus grands établissements médicaux-sociaux du canton de Genève. | Photo emsvessy.ch

C'est un témoignage rare et précieux. Au mois de septembre, l'établissement médico-social Maison de Vessy a été victime d'une cyberattaque. Que s'est-il passé? *Heidi.news* a contacté l'institution pour lui proposer de témoigner sur cet événement. Florence Moine, directrice générale de l'EMS, a accepté de se livrer à l'exercice.

Pourquoi c'est intéressant. Maison de Vessy est un établissement public autonome de 300 collaborateurs pour 226 lits. La moyenne d'âge des résidents est de 89 ans. C'est l'un des trois plus grands EMS du canton de Genève. Compte tenu de son importance, l'institution dispose d'un piquet technique 24 heures sur 24 et 7 jours sur 7. Les institutions médicales sont des cibles privilégiées pour les pirates malveillants. En bloquant l'accès à des données médicales sensibles, les assaillants espèrent que les victimes obtempéreront plus facilement pour retrouver la maîtrise de leurs systèmes informatiques.

Ce qu'il s'est passé. La cyberattaque a été découverte le dimanche 12 septembre. Un infirmier qui rencontrait des problèmes de connexion au dossier informatisé d'un résident a contacté le service technique qui a contacté le prestataire informatique. Ce dernier a immédiatement constaté des anomalies, certaines pouvant faire penser à une intrusion malveillante dans les systèmes informatiques. Les serveurs ont

été débranchés physiquement pour les protéger d'une propagation virale de l'attaque. «Nous avons dès lors mis en place un plan de continuité au niveau du comité de direction, explique Florence Moine, pour passer en mode "dégradé" en termes de communication et de poursuite de l'activité de l'EMS.»

Les systèmes informatiques de Maison de Vessy ont été la cible d'un rançongiciel, c'est-à-dire un logiciel malveillant qui bloque l'accès aux données afin d'exiger une rançon aux victimes qui veulent récupérer la maîtrise de leurs outils. En l'occurrence, le rançongiciel a infecté l'EMS a chiffré les données et en a soustrait une partie. Sur les 26 serveurs de l'institution, 16 d'entre eux ont été chiffrés, sauvegardes comprises, et trois serveurs ont été détruits. En tout, plus de 50'000 fichiers ont été chiffrés et potentiellement exfiltrés. Ils contenaient des données médicales, sociales ou encore financières.

Les pirates malveillants à l'origine de l'attaque ont exigé une rançon, que l'EMS a refusé de payer, comme le recommandent les autorités. Des informations ont été soustraites par les assaillants, et rien ne garantit que les données ne seront pas exploitées ultérieurement.

Les conséquences de l'attaque. Toutes les données ont pu être récupérées grâce à une sauvegarde externe hors ligne, datant du 25 août. Florence Moine revient sur cette période:

«La saisie manuelle visant à rétablir les 15 jours manquants nous a valu des heures de travail supplémentaires, mais nous n'avons objectivement perdu aucune donnée et nous avons toujours fonctionné. Certes, avec papier et stylo, mais sans danger aucun pour la prise en charge des résidents.»

Pour des questions de sécurité, les réseaux virtuels privés qui relient l'EMS à certains partenaires privilégiés – HUG et pharmacies – ont dû être coupés. Il n'était pas possible de rétablir ces connexions tant que les systèmes informatiques de Maison de Vessy n'étaient pas sécurisés. Conséquence directe: des collaborateurs de l'EMS ont dû se rendre aux HUG pour faire de la saisie d'informations.

Des données personnelles des collaborateurs ayant potentiellement été soustraites – montant du salaire, contrat de travail, etc. –, cela a généré des inquiétudes. «Nous nous sommes rendus disponibles immédiatement pour les collaborateurs qui pouvaient nourrir des craintes, raconte Florence Moine. Nous avons fortement collaboré avec la commission du personnel pour que celle-ci serve de relais d'alerte et avons mis un point d'honneur à leur répondre dans les heures qui suivaient une demande de leur part.» Les cadres de l'institution sont restés disponibles en tout temps pour recevoir

d'éventuels collaborateurs ayant besoin d'échanger sur cet événement ou d'être rassurés à titre personnel.

Une cellule de soutien pour les résidents et les proches. Face à l'ampleur de l'attaque, la direction de Maison de Vessy a mis en place une cellule de soutien pour les résidents et les proches. Florence Moine raconte avoir «demandé au comité de direction, moi y compris, de poser le stylo et de prendre tous les appels en direct pour assumer la crise et la réponse de première ligne. C'était le minimum dû aux résidents, aux familles et aux collaborateurs: s'excuser et compatir au stress de l'interlocuteur, écouter, répondre factuellement et de façon la plus pédagogique possible, conseiller au mieux, rester disponible pour la suite.»

L'EMS a diffusé un communiqué informant de l'attaque dont il a été victime le 20 septembre, soit environ une semaine après. Florence Moine explique ce timing, qu'elle juge «à la fois très court et très long»:

«C'est difficile de communiquer tout de suite, tant qu'on n'a pas suffisamment d'informations factuelles et que l'on est encore au stade des hypothèses concernant l'attaque, son périmètre et ses enjeux. Communiquer quand on n'a rien de fiable sur quoi s'appuyer est risqué et compliqué vis-à-vis d'une population que l'on sait être fragile. On voudrait pouvoir rassurer, ce qui est quasiment impossible, mais ne pas communiquer est toujours pire.»

Impensable pour la direction de ne pas partager la situation avec les résidents et leurs proches, ce d'autant plus que des données personnelles qui les concernent ont pu être potentiellement volées. «La relation de confiance voulue avec les résidents et leurs proches passe par une transparence non négociable.»

En dix jours, la cellule de soutien a reçu 27 appels téléphoniques de familles et de proches de résidents de l'EMS. «Ces personnes ont toutes fait preuve d'une incroyable compréhension face à cet incident», souligne Florence Moine. Les familles et les proches qui ont contacté l'institution voulaient principalement connaître les impacts que pouvaient avoir cette attaque sur eux. La directrice générale explique:

«Nous avons conseillé du mieux que nous pouvions: installer un mot de passe robuste sur l'informatique personnel, prévenir sa banque de la cyberattaque en lui partageant notre courrier, ne jamais répondre à un mail qui semblerait provenir de Maison de Vessy.»

L'EMS a mis en place, avec la société de cybersécurité mandatée pour l'accompagner durant la crise, une veille quotidienne du

darkweb pour identifier au plus vite d'éventuelles fuites d'informations liées à l'institution.

Les conseils de Florence Moine en cas de cyberattaque. La directrice générale de Maison de Vessy estime qu'il est important, en cas d'attaque informatique, de s'entourer immédiatement d'experts dans le domaine de la gestion de crise. «Que cela soit des communicants, des avocats ou encore des spécialistes de l'informatique, ces personnes pourront vous soutenir et vous conseiller.» Elle ajoute qu'il faut s'appuyer sur tous les cadres de l'institution. «Une telle crise se traverse en équipe.» Enfin, elle souligne l'importance de la transparence – tant à l'interne qu'à l'externe. «On nous pardonnera d'avoir eu un incident, mais pas de l'avoir dissimulé, et à juste titre», conclut-elle.

Cybersécurité **Cyberattaque** **EMS** **Maison De Retraite** **Protection Des Données**