La cybersécurité dans le secteur de la santé, un enjeu prioritaire

En mars et avril dernier, en pleine crise sanitaire, une cyberattaque visant les systèmes informatiques du secteur de la santé a eu lieu tous les trois jours dans le monde. Dans ce contexte critique, une tribune internationale, signée par plusieurs prix Nobel de la paix, des anciens présidents ainsi que des présidents d'ONG a appelé fin mai les Etats à tout mettre en oeuvre pour sécuriser leurs systèmes de santé, en y allouant des ressources technologiques et financières suffisantes.

Les données recueillies dans le secteur de la santé sont particulièrement sensibles. Les organismes de soin sont des cibles de choix pour les cybercriminels qui cherchent à obtenir des informations précieuses en exploitant des systèmes de sécurité vulnérables. Afin de réduire les risques, les mesures de sécurité adoptées doivent inclure des méthodes d'authentification forte, la formation des employés et la communication avec ceux-ci, ainsi qu'une extension des mesures de cybersécurité à la chaîne d'approvisionnement de l'organisation.

Dans ce secteur en particulier, les systèmes informatiques contiennent des données sensibles et appuient les organismes dans la prestation de services de qualité aux patients, ce qui fait en fait une cible de choix pour les tentatives d'extorsion. Le phishing, par lequel un cybercriminel se présente comme une organisation ou un individu légitime afin de piéger une cible, est une forme d'attaque fréquemment utilisée. Les emails constituent souvent un point d'entrée, car ils contiennent des liens vers de faux sites web ou de fausses pièces jointes.

Ce type d'attaque est particulièrement préoccupant dans le domaine des soins de santé, dans la mesure où il peut compromettre les comptes de messagerie électronique utilisés pour échanger des données hautement sensibles. Si les informations de connexion à la messagerie électronique d'un employé sont dérobées ou divulguées mdash; y compris son nom d'utilisateur et son mot de passe - elles peuvent être utilisées par des criminels pour accéder aux informations relatives aux patients.

Les organismes de santé doivent veiller à mettre en place des mesures de sécurité rigoureuses afin de limiter les risques de compromission des comptes de messagerie, de violation des données et d'autres incidents de cybersécurité. Il convient de noter que ces mesures doivent couvrir tous les paramètres inhérents aux personnes, aux processus et aux technologies :

Pratiques et procédures - méthodes d'authentification forte, accès sécurisé aux applications, aux systèmes et aux données ;
Communication avec le personnel et les autres parties prenantes clés - mises à jour régulières, ainsi que rappels des comportements à adopter en matière de sécurité et des mesures obligatoires à prendre en cas de défaillance de la sécurité ;
Relations avec les fournisseurs - les cybercriminels peuvent exploiter tout maillon faible d'une chaîne d'approvisionnement pour accéder à une cible. Selon Osterman Research : « L'existence de liens étroits entre les entreprises au sein d'un écosystème de soins de santé peut compromettre tout un écosystème » ;
Formation - formation à l'entrée en service, rappels réguliers et formation complémentaire pour l'ensemble du personnel et, le cas échéant, d'autres parties prenantes.

Une authentification plus forte pour améliorer la sécurité

Le moyen utilisé par les employés pour authentifier leur identité afin d'accéder à leur messagerie électronique, à d'autres applications fondées sur le cloud et aux systèmes informatiques est une des principales voies d'accès pour les criminels. Il est donc indispensable que les organisations qui cherchent à protéger leurs employés et leurs actifs contre les effets nuisibles du phishing et d'autres attaques visant à compromettre les identifiants de connexion aient recours à l'authentification à plusieurs facteurs (MFA).

Avec la MFA, les utilisateurs doivent fournir plus que des éléments dont ils ont connaissance (un identifiant/mot de passe). Ainsi, ils peuvent renseigner un facteur qu'ils possèdent, comme un dispositif d'authentification physique, et/ou un élément qui leur est propre - qui peut prendre la forme d'un identifiant biométrique comme une empreinte digitale ou un scan de l'iris.

L'option d'authentification la plus forte repose sur une clé de sécurité, laquelle peut être associée aux applications et services utilisés par les employés. Chaque fois qu'un collaborateur tente de se connecter, une clé de sécurité est également requise pour accéder à l'application, ce qui permet de garantir un niveau de protection bien plus élevé qu'une simple combinaison de nom d'utilisateur et de mot de passe. La clé de sécurité, qui est un élément dont dispose un employé, vient s'ajouter à l'élément qu'il connaît. Et, comme l'authentification ne repose plus uniquement sur cet élément connu - qui peut être volé par une attaque de phishing - la sécurité est ainsi renforcée.

Il est primordial que les organisations de tous les secteurs adoptent des mesures de cybersécurité solides. Les organismes de santé constituent une cible de choix pour les cybercriminels en raison de la nature très sensible des données qu'ils détiennent et traitent. Afin de limiter les risques de violation et d'autres incidents compromettant la cybersécurité, ils doivent mettre en place des procédures de sécurité claires et efficaces, ainsi que des méthodes d'authentification forte. Cette approche devrait s'accompagner d'une communication et d'une formation régulières afin que la cybersécurité soit non seulement appliquée dans la pratique, mais qu'elle constitue également le fondement d'une culture au sein de l'organisation et au-delà.