La formation des employés, seule solution contre le phishing dans le secteur de la santé ?

L'Association pour la sécurité des systèmes d'information de santé (APSSIS) a publié début juin un « panorama des arnaques et attaques » informatiques utilisant le Covid-19 « pour tenter de soutirer de l'argent ou des données aux victimes potentielles ». Elle recense ainsi sept types d'arnaques et d'attaques, dont la première est le phishing. Les cyberattaques perpétrées à l'encontre des organismes dans le secteur de la santé ont fortement augmenté au cours des derniers mois. Les cybercriminels ont en effet profité de la crise sanitaire liée au Covid-19 pour multiplier leurs actions. L'AP-HP en a notamment fait les frais, victime d'une attaque par déni de service (DDoS) en mars dernier.

Pour lutter contre les cyberattaques, et plus particulièrement le phishing, les organismes de santé ont tout intérêt à prendre les mesures nécessaires afin de réduire le cyber-risque et de limiter les préjudices potentiels. Mais la question est de savoir dans quelle mesure ces méthodes sont efficaces et quelle approche les établissements doivent-ils adopter pour éviter la compromission de données sensibles en cas d'attaques.

La santé, secteur privilégié des attaques de phishing

Il existe plusieurs raisons pour lesquelles les attaques de phishing ciblent si souvent les organismes de soins de santé. Tout d'abord, elles affichent un taux de réussite élevé. Il suffit en effet d'une seule erreur - un employé qui se laisse duper en cliquant sur un lien malveillant - pour que le malfaiteur s'introduise dans le réseau. De plus, certaines attaques de ce type, appelées « spear-phishing », sont soigneusement conçues pour cibler des utilisateurs précis, ce qui augmente la probabilité que ces derniers ouvrent l'email et cliquent sur les liens malveillants qu'il contient.

En outre, les pirates sont particulièrement enclins à cibler les établissements de ce secteur car les données de santé personnelles qu'ils stockent sont très précieuses. Selon l'organisation américaine Center for Internet Security (CIS), un dossier médical peut se vendre sur le marché noir à hauteur de 363 dollars, alors que les informations d'identification personnelle (IIP) se vendent seulement à 1 ou 2 dollars. Cette différence de coût s'explique par une raison simple : les criminels peuvent facilement utiliser les dossiers médicaux à des fins de fraude, de vol d'identité ou d'extorsion, et les victimes ne sont pas en mesure de rendre ces dossiers inutilisables aussi facilement qu'elles peuvent bloquer un numéro de carte de crédit ou fermer un compte bancaire.

Réduire les chances de réussite d'une attaque de phishing

La première étape dans la lutte contre les attaques de phishing consiste à dispenser une formation complète aux employés et à tester régulièrement la façon dont chacun a intégré les enseignements. De nombreux organismes de santé intensifient leurs efforts dans ce domaine. Aussi, d'après le rapport Netwrix 2020 IT Trends, 56 % des établissements dans ce secteur considèrent en effet le renforcement de la sensibilisation à la cybersécurité comme l'une de leurs principales priorités. La deuxième étape essentielle consiste à mettre en oeuvre des politiques plus rigoureuses en matière de sécurité, notamment en ce qui concerne la sécurité des emails et la complexité des mots de passe. Il est préférable de ne pas attendre de subir une violation de données pour revoir soigneusement ses politiques et les mettre à jour afin de tenir compte des meilleures pratiques en

vigueur.

Bien que ces mesures contribuent à réduire les chances de réussite d'une attaque de phishing, elles ne garantissent pas une protection absolue des données. Il existe toujours un risque qu'un employé néglige sa formation et clique sur un lien dans un email de phishing mdash; surtout s'il s'agit d'un message particulièrement convaincant. Outre la menace liée au phishing, il est également primordial de surveiller en permanence les potentielles activités suspectes des utilisateurs dans l'ensemble de l'environnement informatique sur site, dans le cloud ou hybride. Cela implique pour les organismes de santé d'avoir une visibilité complète des données de leurs patients, quel que soit l'endroit où elles se trouvent, afin de limiter le risque de compromission.

Des mesures clés et incontournables pour se protéger

Si un organisme de santé décide de dispenser une formation complète aux utilisateurs et de renforcer ses politiques de sécurité pour bloquer le plus grand nombre d'attaques possible, il doit également adopter des mesures qui l'aideront à détecter et à enquêter rapidement sur les attaques de phishing fructueuses et les comportements suspects des utilisateurs. Pour limiter les pertes financières, les violations de la réglementation ainsi qu'une dégradation de sa réputation et de son image, un établissement de santé doit être en mesure d'arrêter les cybercriminels avant qu'ils ne compromettent d'importants volumes de données de patients.

Pour y parvenir, il est primordial de surveiller les activités des utilisateurs et de bien comprendre ce qui se passe dans l'environnement IT ; notamment de savoir qui modifie ou copie quelles données personnelles de santé. En étant capables de détecter des activités inhabituelles susceptibles de compromettre les données des patients et de procéder rapidement à une enquête, les organismes de santé pourront prendre les mesures nécessaires avant de subir une violation de données. Dans l'idéal, il est souhaitable de définir des alertes automatiques en cas d'événements suspects, comme de multiples tentatives de connexion infructueuses ou une personne qui accède à des informations médicales qu'elle n'a jamais consultées auparavant.

De plus, il est nécessaire de procéder à un examen régulier et de réduire au minimum les autorisations. Un cybercriminel qui compromet les informations d'identification d'un employé peut accéder à toutes les données sensibles accessibles via son compte. Il s'agit donc d'une pratique fondamentale pour veiller à ce que chaque utilisateur ne dispose que des privilèges minimaux dont il a besoin pour effectuer son travail. Par exemple, un assistant ne devrait pas avoir accès aux données sensibles des patients. L'application rigoureuse du principe du moindre privilège, accompagnée de révisions régulières des autorisations, réduira considérablement la surface d'attaque. Accorder une attention particulière aux utilisateurs privilégiés est également primordial, car les pirates informatiques essaient bien souvent d'obtenir leurs informations d'identification. Il faut en particulier s'assurer que les utilisateurs privilégiés ne disposent pas d'un accès universel à l'ensemble des systèmes et des stockages de données (par exemple, un compte administrateur SQL ne devrait pas être membre du groupe d'administrateurs de domaines).

Enfin, si les organismes de santé connaissent le type de données qu'elles stockent, à quel endroit et les personnes qui y ont accès, ils peuvent déterminer les données qui nécessitent une attention particulière et mettre en place des contrôles appropriés pour se protéger. Dans ce cadre, la classification des données pour évaluer les risques associés aux données personnelles de santé est un très bon outil. Pour réduire davantage le risque de violation des données personnelles de santé, il est par ailleurs essentiel d'appliquer les bonnes pratiques de base pour améliorer son niveau de sécurité général, comme la mise à jour des correctifs logiciels, le chiffrement des données sensibles et l'utilisation de logiciels antivirus.

Afin de lutter efficacement contre les menaces liées au phishing et de protéger leurs données, les

organismes de santé doivent impérativement disposer d'une stratégie de défense solide. Les principaux éléments comprennent une formation régulière à la cybersécurité, l'application du principe du moindre privilège pour les utilisateurs réguliers et les administrateurs, et la classification des données afin de prioriser les efforts de protection des données et se conformer aux exigences réglementaires ; un enjeu majeur et accru sur fond de crise sanitaire.