Scénario

Une petite clinique américaine spécialisée dans les soins de santé primaires a été victime d'un incident de sécurité un mardi matin, vers 9 heures. Plusieurs employés ont signalé qu'ils n'arrivaient pas à accéder à des fichiers depuis leurs ordinateurs, notamment des dossiers médicaux. Les activités de l'entreprise ont été interrompues parce que les employés n'ont pas pu accéder aux fichiers et aux logiciels dont ils avaient besoin pour faire leur travail.

De plus, les employés ont également signalé qu'une demande de rançon s'était affichée sur leurs ordinateurs. La demande de rançon indique que tous les fichiers de l'entreprise ont été chiffrés par un groupe organisé de pirates informatiques sans scrupules, connus pour cibler les entreprises des secteurs de la santé et des transports. Pour rétablir l'accès aux fichiers chiffrés, la note de rançon exige une forte somme d'argent en échange de la clé de déchiffrement.

Les pirates ont pu accéder au réseau de l'entreprise en utilisant des e-mails d'hameçonnage ciblés, qui ont été envoyés à plusieurs employés de l'entreprise. Les e-mails d'hameçonnage contenaient une pièce jointe malveillante qui, une fois téléchargée, installait un logiciel malveillant sur l'ordinateur de l'employé.

Une fois l'accès obtenu, les pirates ont déployé leur rançongiciel, qui a chiffré les fichiers critiques. L'entreprise n'a pas pu accéder aux données critiques des patients, ce qui a entraîné des perturbations majeures dans ses activités. Elle a été contrainte de mettre ses systèmes informatiques hors service et de contacter plusieurs organismes pour signaler l'incident et recevoir une assistance technique.