Quand le cabinet est soudainement hors ligne. Rapport d’un cybersinistre réel.

En théorie, de nombreux propriétaires de cabinet médical savent qu'une cyberattaque peut survenir à tout moment. Malgré cela, de nombreuses personnes pensent que ce sont plutôt d'autres entreprises qui sont menacées et elles espèrent ne pas être concernées elles-mêmes. Mais que faire si votre propre cabinet est soudainement attaqué ? C'est exactement ce qu'a vécu un cabinet médical qui, malgré les mesures de sécurité prises, a été victime d'une attaque de ransomware. Nous avons parlé de ce cas avec la compagnie d'assurance responsable et nous montrons comment une cyberassurance peut aider en cas d'urgence.

En fin d'après-midi, personne n'a d'abord remarqué que des cybercriminels avaient accédé aux configurations centrales des serveurs du cabinet. Ce n'est que le lendemain matin qu'on s'est aperçu que des fichiers système essentiels, nécessaires au démarrage et au chargement des serveurs, avaient été chiffrés. Il s'agissait d'une attaque classique de ransomware : les criminels ont laissé une « ransom note », c'est-à-dire un message numérique de chantage invitant à les contacter. Il n'y avait pas de demande concrète de rançon. L'objectif des auteurs était toutefois clair : négociation et paiement.

L'entreprise sous pression - mais aucune donnée de patient concernée
Malgré les circonstances, les activités du cabinet ont pu être maintenues, mais les activités informatiques étaient limitées. Par exemple, les médecins traitants n'ont pu documenter leurs consultations et les saisir dans le système informatique qu'a posteriori. La gestion organisationnelle et technique de la situation était également un surcroît de travail. Au total, la charge de travail interne supplémentaire du cabinet s'est élevée à environ 60 heures. Heureusement, les données des patients n'ont pas été concernées par le chiffrage. Il n'a pas non plus été possible de démontrer une fuite de données. Les analyses de l'informatique légale ont montré, sur la base des temps d'accès, qu'un vol complet des données médicales était très improbable.

Une aide rapide grâce à l'assurance et aux spécialistes
Après avoir pris connaissance de l'attaque, le cabinet a agi immédiatement et il a informé son prestataire de services informatiques. Parallèlement, la cyberassurance a été contactée et elle a immédiatement réagi en mettant à disposition, dans les plus brefs délais, un expert en sécurité informatique spécialisé dans la réaction aux incidents et la criminalistique. Il a aidé le cabinet lors de l'analyse technique, il a aidé à restaurer les systèmes de manière ordonnée et il a fourni des recommandations afin de renforcer la sécurité informatique. Un soutien juridique a également été organisé : un avocat spécialisé dans le droit de la protection des données a aidé à clarifier les obligations de déclaration.

Il n'y a pas eu de communication ni de négociation avec les extorqueurs, car les spécialistes en informatique ont pu rétablir l'environnement informatique dans un délai raisonnable. Grâce à l'action coordonnée de toutes les parties concernées, la restriction informatique a pu être limitée à deux jours. Pendant cette période, le fonctionnement du cabinet médical était plus difficile, mais pas complètement paralysé, et les patients ont pu continuer à être traités.

Prise en charge des coûts par la cyberassurance
Le préjudice financier total s'est élevé à environ 25 000 francs suisses. La plus grande partie a été consacrée aux différents travaux informatiques, qui ont coûté environ 18 000 francs. S'y sont ajoutés des coûts supplémentaires internes d'environ 5 000 francs suisses ainsi que des frais de conseil juridique d'environ 2 000 francs suisses. L'assurance a pris en charge tous les frais après la déduction de la franchise. Le préjudice financier pour le cabinet s'est donc limité à la franchise grâce à la cyberassurance.

Conclusion
Ce cas illustre parfaitement la rapidité avec laquelle un cabinet peut être dans une situation grave et à quel point le soutien de partenaires spécialisés est précieux. Alors que le grand public ne parle souvent que d'attaques de grande envergure, ce sont en réalité souvent des petites et moyennes entreprises, comme les cabinets médicaux, qui sont concernées. Il est donc d'autant plus

important d'être bien préparé, que ce soit par des mesures de sécurité techniques, des procédures claires en cas d'urgence et aussi une assurance qui ne se contente pas de payer en cas de sinistre, mais qui apporte un soutien actif.

Votre cabinet est-il suffisamment protégé ?
Les cyberattaques peuvent concerner n'importe quel cabinet, même avec des mesures de sécurité minutieuses en place. Nous vous conseillons volontiers personnellement et vous soumettons une offre sans engagement - gratuitement et en fonction de votre situation individuelle. Appelez-nous au 031 959 50 00 ou consultez notre site internet à l'adresse www.fmhinsurance.ch/cyber.

FMH Services (Insurance)
Roth Gygax & Partner AG*
Moosstrasse 2
3073 Gümligen
Téléphone 031 959 50 00
mail@fmhinsurance.ch
www.fmhinsurance.ch

*Roth Gygax & Partner AG est une entreprise de conseil indépendante sur le plan juridique et économique recommandée par la société coopérative FMH Services.