

Protection contre l'ingénierie sociale et le piratage social

Dans un monde de plus en plus numérisé, les médecins et leurs cabinets dépendent de plus en plus de la disponibilité de données et de systèmes numériques. Parallèlement, le risque de cyber-attaques ne cesse d'augmenter. Un domaine qui est souvent sous-estimé est celui de l'ingénierie sociale et du piratage social. Pour ce faire, le hacker exploite de manière ciblée les faiblesses humaines afin d'obtenir des informations sensibles. Cet article définit les grandes lignes sur le sujet et montre comment vous pouvez vous protéger.



Qu'est-ce que l'ingénierie sociale et le piratage social?

L'ingénierie sociale désigne la manipulation de personnes afin de les amener à révéler des informations confidentielles ou à effectuer certaines actions qui avantagent le hacker. Cela peut se faire par exemple par des e-mails de phishing, des appels téléphoniques falsifiés ou des interactions sur les réseaux sociaux. Le piratage social, quant à lui, fait référence à l'utilisation abusive des interactions sociales pour accéder à des systèmes ou à des données sensibles, que ce soit par la manipulation, la tromperie ou l'influence directe.

Les dangers pour les cabinets médicaux

L'ingénierie sociale et le piratage social sont particulièrement menaçants pour les cabinets médicaux qui disposent de données sensibles sur les patients et d'informations confidentielles. Une attaque réussie peut non seulement entraîner des fuites de données, mais aussi ébranler la confiance des patients et nuire gravement à la réputation du cabinet et du médecin. En outre, des pertes financières peuvent résulter de fraudes ou d'extorsions.

Le rôle de la cyber-assurance

Les cyber-assurances jouent un rôle important dans la protection contre les conséquences des cyber-attaques. D'une part, l'assurance offre une protection financière en cas de cyber-événement. D'autre part, les cyber-assurances proposent différents services en cas de sinistre, comme une hotline 24h/24 et des enquêtes médico-légales, ainsi que d'autres en matière de prévention des sinistres.

Étendue de la couverture d'assurance

Notre cyber-assurance, spécialement conçue pour répondre aux besoins du corps médical, couvre aussi bien les dommages personnels que les dommages en responsabilité civile. Les dommages propres couvrent, par exemple, les coûts de restauration du système après une attaque. En outre, l'assurance prend en charge la perte de revenus lorsqu'un cabinet médical doit être fermé, par exemple parce qu'il n'est pas possible d'accéder aux dossiers des patients. Par dommages en responsabilité civile, l'on entend les prétentions de tiers, par exemple lorsqu'il n'est plus possible d'accéder à un résultat de laboratoire et que l'examen doit être refait, ou les dommages résultant d'une violation de la protection des données. En plus de la couverture de base, l'ingénierie sociale et le piratage social peuvent être assurés moyennant une surprime. En outre, les manipulations de la banque en ligne ou de l'installation téléphonique peuvent également être assurées et le paiement de la rançon peut être choisi en option.

Service de prévention

Outre la couverture d'assurance, il est crucial de prendre des mesures préventives pour se prémunir contre les attaques d'ingénierie sociale. C'est pourquoi notre cyber-assurance pour médecins comprend un service de prévention gratuit. Les cabinets médicaux peuvent ainsi former et sensibiliser leur personnel à la cyber-sécurité. En outre, le service de prévention comprend différents conseils pour augmenter la sécurité du système.

En résumé

L'ingénierie sociale et le piratage social constituent des menaces sérieuses pour les cabinets médicaux, car ils exploitent les faiblesses humaines afin d'accéder à des informations sensibles. Les cyber-assurances jouent un rôle important dans la protection contre les conséquences financières de telles attaques. Elles offrent la sécurité et la protection

dont vous avez besoin pour protéger les données de vos patients et votre réputation. Grâce à des mesures préventives et à des formations, vous pouvez en outre contribuer à vous défendre contre les attaques d'ingénierie sociale et à renforcer votre cybersécurité.

Exemple pratique d'ingénierie sociale

Une femme appelle un cabinet médical pour prendre rendez-vous afin de présenter une nouvelle solution logicielle. Anna, l'assistante médicale, refuse car elle est très satisfaite du logiciel utilisé. Au moment de partir de l'entreprise, Peter s'intéresse à la solution informatique qui est utilisée en interne. Quelques semaines plus tard, un homme du nom de Martin appelle le même cabinet médical. Il prétend qu'une mise à jour de sécurité urgente est nécessaire pour le logiciel qu'utilise au cabinet et qu'il doit venir en personne pour l'installer. Martin sait quelle solution logicielle le cabinet médical utilise et le numéro qui s'affiche sur l'écran d'Anna correspond également à la société de logiciels. Martin raconte que la mise à jour doit être installée rapidement afin de corriger des vulnérabilités critiques et de protéger les données sensibles des patients. Anna s'inquiète de la sécurité des données des patients et prend l'appel de Martin au sérieux. Bien qu'elle n'ait pas reçu d'instructions spécifiques de son supérieur, qui se trouve malheureusement à un congrès, elle veut garantir la sécurité du cabinet et accepte la visite de Martin. Le jour même, Martin se présente au cabinet et est accueilli chaleureusement par Anna. Il porte une veste avec le logo de la célèbre entreprise de logiciels et a sur lui un sac contenant un ordinateur portable et divers câbles. Anna le conduit à une salle de soins libre où il peut faire son travail. Alors que Martin prétend installer la mise à jour de sécurité, il en profite pour accéder discrètement aux ordinateurs et au réseau du cabinet. Il installe secrètement un logiciel d'accès à distance qui lui permet d'accéder ultérieurement aux systèmes depuis l'extérieur. Après avoir terminé sa prétendue mise à jour, Martin remercie Anna et quitte le cabinet. Anna, soulagée par l'installation de la mise à jour, retourne à son poste de travail et part du principe que les données des patients sont désormais en sécurité. Ce qu'Anna ne soupçonne pas, c'est que le groupe de hackers a déjà commencé à voler les données des dossiers des patients. Deux jours plus tard, une demande de chantage arrive dans la boîte aux lettres électronique. Si le cabinet ne transfère pas la demande de rançon dans les 48 heures, les données du patient seront publiées sur le dark web. Pour preuve, quelques dossiers de patients sont joints à l'e-mail. Cet exemple illustre comment l'ingénierie sociale peut aboutir à ses fins même dans un environnement de confiance tel qu'un cabinet médical, lorsque les employés ne sont pas suffisamment formés ou sous-estiment l'importance des mesures de sécurité.

A propos

Roger Ledermann

Spécialiste en assurance, Planificateur financier avec le brevet fédéral

FMH Services (Insurance)

Roth Gyax & Partner AG*

Moosstrasse 2

3073 Gümligen

Téléphone 031 959 50 00

mail@fmhinsurance.ch

www.fmhinsurance.ch

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