FMH SERVICES

Schutz vor Social Engineering und Social Hacking

In einer zunehmend digitalisierten Welt sind Ärzte und deren Praxen vermehrt auf die Verfügbarkeit von digitalen Daten und Systemen angewiesen. Gleichzeitig steigt die Gefahr von Cyberangriffen stetig. Ein Bereich, der dabei oft unterschätzt wird, ist das sogenannte Social Engineering und Social Hacking. Dabei nutzt der Angreifer gezielt menschliche Schwächen aus, um an sensible Informationen zu gelangen. Dieser Artikel wirft einen Blick auf dieses Thema und zeigt auf, wie Sie sich gegen die Folgen schützen können.

Was ist Social Engineering und Social Hacking?
Social Engineering bezeichnet die Manipulation von Menschen, um sie dazu zu bringen, vertrauliche Informationen preiszugeben oder bestimmte Handlungen auszuführen, die für den Angreifer von Vorteil sind. Dies kann beispielsweise durch Phishing-E-Mails, gefälschte Anrufe oder Social-Media-Interaktionen geschehen. Social Hacking hingegen bezieht sich auf den Missbrauch sozialer Interaktionen, um Zugang zu Systemen oder sensiblen Daten zu erlangen, sei es durch Manipulation, Täuschung oder direkte Einflussnahme.

Die Gefahren für Arztpraxen
Für Arztpraxen sind Social Engineering und Social Hacking besonders bedrohlich, da sie über sensible Patientendaten und vertrauliche Informationen verfügen. Ein erfolgreicher Angriff kann nicht nur zu Datenlecks führen, sondern auch das Vertrauen der Patienten erschüttern und den Ruf der Praxis und des Arztes schwer beschädigen. Darüber hinaus können finanzielle Verluste durch Betrug oder Erpressung entstehen.

Die Rolle von Cyberversicherungen
Cyberversicherungen spielen eine wichtige Rolle beim Schutz vor den Folgen von Cyberangriffen. Einerseits bietet die Versicherung einen finanziellen Schutz im Falle eines Cyberereignisses. Andererseits bieten die Cyberversicherungen auch verschiedene Dienstleistungen im Schadenfall wie eine 24-Stunden Hotline und forensische Untersuchungen oder aber auch in der Schadenprävention.

Umfang des Versicherungsschutzes
Unsere Cyberversicherung, welche speziell auf die Bedürfnisse der Ärzteschaft ausgerichtet ist, deckt sowohl Eigenschäden wie auch Haftpflichtschäden. Unter Eigenschäden sind beispielsweise die Kosten für Wiederherstellung des Systems nach einem Angriff abgedeckt. Weiter übernimmt die Versicherung auch den Ertragsausfall, wenn eine Arztpraxis geschlossen bleiben muss, weil zum Beispiel kein Zugriff auf die Patientendossiers vorhanden ist. Unter Haftpflichtschäden versteht man Ansprüche Dritter, wenn beispielsweise kein Zugriff mehr auf einen Laborbefund besteht und dieser deshalb nochmals gemacht werden muss oder Schäden infolge Datenschutzverletzungen. Nebst der Grunddeckung kann Social Engineering und Social Hacking gegen eine Mehrprämie mitversichert werden. Zudem sind auch Manipulationen am E-Banking oder an der Telefonanlage versicherbar und die Zahlung von Lösegeldforderungen ist optional wählbar.

Präventionsservice
Neben dem Versicherungsschutz ist es entscheidend, präventive Massnahmen zu ergreifen, um sich gegen Social Engineering-Angriffe zu wappnen. Deshalb beinhaltet unsere Ärzte-Cyberversicherung einen kostenlosen Präventionsservice. Damit können Arztpraxen ihr Personal schulen und sensibilisieren, um das Bewusstsein für Cybersicherheit zu erhöhen. Zudem umfasst der Präventionsservice verschiedene Tipps, um die Systemsicherheit zu erhöhen.

Fazit
Social Engineering und Social Hacking stellen ernsthafte Bedrohungen für Arztpraxen dar, da sie menschliche Schwächen ausnutzen, um Zugang zu sensiblen Informationen zu erlangen. Cyberversicherungen spielen eine wichtige Rolle beim Schutz vor den finanziellen Folgen solcher Angriffe und bieten die Sicherheit und den Schutz, den Sie benötigen, um ihre Patientendaten und ihren Ruf zu schützen. Durch präventive Massnahmen und Schulungen können Sie zusätzlich dazu beitragen, sich gegen Social Engineering-Angriffe zu verteidigen und ihre Cybersicherheit zu stärken.

Praxisbeispiel Social Engineering

Eine Frau ruft eine Arztpraxis an, um einen Termin für eine Vorstellung einer neuen Softwarelösung zu vereinbaren. Die Praxisassistentin Anna lehnt ab, da sie mit der eigesetzten Software sehr zufrieden ist. Beim Verabschieden erkundigt sich die Frau interessenhalber, welche Lösung denn eingesetzt werde. Einige Wochen später ruft ein Mann namens Martin die gleiche Arztpraxis an. Er behauptet, dass es ein dringendes Sicherheitsupdate für die verwendete Praxissoftware gibt und dass er persönlich vorbeikommen müsse, um es zu installieren. Martin weiss, welche Softwarelösung die Arztpraxis einsetzt und auch die Nummer, welche im Display von Anna angezeigt wird, passt zur Softwarefirma. Martin erzählt, dass das Update schnell installiert werden müsse um kritische Schwachstellen zu beheben und sensible Patientendaten zu schützen. Anna ist besorgt über die Sicherheit der Patientendaten und nimmt Martins Anruf ernst. Sie hat zwar von ihrem Vorgesetzten, welcher an einem Kongress weilt, keine spezifischen Anweisungen erhalten, will die Sicherheit der Praxis aber gewährleisten und stimmt Martins Besuch zu. Noch am selben Tag erscheint Martin in der Praxis und wird von Anna freundlich begrüsst. Er trägt eine Jacke mit dem Logo des bekannten Softwareunternehmens und hat eine Tasche mit Laptop und verschiedenen Kabeln bei sich. Anna führt ihn zu einem freien Behandlungszimmer, in dem er seine Arbeit verrichten kann. Während Martin vorgibt, das Sicherheitsupdate zu installieren, nutzt er die Gelegenheit, um sich unauffällig Zugang zu den Computern und dem Netzwerk der Praxis zu verschaffen. Er installiert heimlich eine Remote-Zugriffssoftware, die es ihm ermöglicht, später von extern auf die Systeme zuzugreifen. Nachdem Martin sein angebliches Update abgeschlossen hat, bedankt er sich bei Anna und verlässt die Praxis. Anna, erleichtert
über die Installation des Updates, geht zurück an ihren Arbeitsplatz und geht davon aus, dass die Patientendaten jetzt sicher sind. Was Anna zu dem Zeitpunkt noch nicht ahnt, ist dass die Angreifertruppe bereits mit dem Datendiebstahl der Patientenakten begonnen hat. Zwei Tage später geht eine Erpresserforderung im E-Mail Postfach ein. Überweist die Praxis innerhalb von 48 Stunden die Lösegeldforderung nicht, werden die Patientendaten im Darknet veröffentlicht. Zum Beweis sind einige Patientenakten dem E-Mail angefügt. Dieses Beispiel verdeutlicht, wie Social Engineering auch in einer vertrauenswürdigen Umgebung wie einer Arztpraxis erfolgreich sein kann, wenn Mitarbeiter nicht ausreichend geschult sind oder die Bedeutung von Sicherheitsvorkehrungen unterschätzen.

Zur Person

Roger Ledermann
Versicherungsfachmann, Finanzplaner mit eidg. Fachausweis

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

*Die Roth Gygax & Partner AG ist ein von der FMH Services Genossenschaft empfohlenes, rechtlich und wirtschaftlich selbstständiges Beratungsunternehmen.