Die „geheimen Tricks“

im Umgang mit Versicherungen

Teil 22: „Was ist das mit Cyber?“ - Teil II

Was sind die Tricks erfahrener Versicherungsberater im immer schwierigeren Umgang mit den Versicherungsgesellschaften? Die werden natürlich von niemandem verraten - außer eben hier, für alle für Zahnärztinnen und Zahnärzte relevanten Versicherungsbereiche.

Es ist nicht lange her, da hatte man zum Thema Cyberkriminalität vor allem E-Mails der Marke „Nigeria Connection“ im Hinterkopf. Das waren (und ja, tatsächlich: sind) abenteuerliche Geschichten, die der Empfänger des E-Mails aufgetischt bekommt: Afrikanische Prinzen, Präsidentensöhne im Exil oder lange verlorene Verwandte bitten in ausführlichen, teils in wohl formulierten Geschichten und teils in grässlichem Englisch, um Hilfe. Nur etwas Geld bräuchten sie, für Bestechungen und Gebühren, dann könnten sie ihr Millionenvermögen außer Landes schaffen. Zur Belohnung würde der großzügige Helfer aus dem Westen mit einem satten Anteil der geretteten Summe belohnt. Rückblickend betrachtet: Ach, waren das schöne ruhige Zeiten!

© Andrey Popov - Fotolia.com

Der neue Alltag des Verbrechens aus dem Internet

Konnten wir uns früher nicht vorstellen, selbst auf eine solche, übrigens „Vorschussbetrug" genannte, Betrugsmasche hereinzufallen, hat sich das Bedrohungspotential inzwischen völlig verändert. Mit der Nutzung des Internet und elektronisch verarbeiteter Daten in jeder Betriebsform - und nicht zuletzt auch in der Arzt- und Zahnarztpraxis - sind uns all die möglichen Ansätze für das Verbrechen aus dem Internet heute gar nicht mehr bekannt. Erpresser-E-Mails, Virensoftware, Spionagesoftware, die unsere Daten und Bewegungen ausliest, Kreditkartenmissbrauch, Kryptoprogramme, …

Das Internet ist in unserem Leben omnipräsent, und wir dürfen uns daher nicht wundern, dass sich auch das Verbrechen dorthin verlagert hat und uns dort ebenso bedroht wie in der realen Welt.

Reale Cyber-Versicherungsfälle

Wenn jetzt das „Internet der Dinge" in Ihre Ordination Einzug nimmt (oder schon genommen hat), bieten sich nur noch mehr Angriffsflächen - denn das heißt schließlich nichts anderes, als dass auch Ihre Geräte mit einer IP-Adresse ausgestattet sind und als User im world wide web teilnehmen. Userverhalten: noch unbekannt.

Zur Illustration, welche Fälle in unserer Praxis zuletzt aufgetreten sind, haben die Ärzte-Spezialberater unserer Kanzlei eine Auswahl für Sie zusammengestellt.

Fall 1: Gefährliche Mitarbeitersuche

Wer online neue Mitarbeiter sucht, fühlt sich üblicherweise nicht im Fadenkreuz - eher selbst mit Blick durch den Sucher. Aber: Als ein Ordinationsbetreiber gerade auf diversen Plattformen eine neue Assistentin sucht, erhält er eine E-Mail mit einem Anhang „Bewerbung". Die öffnet er, noch erfreut über die rasche Rückmeldung, am Computer in der Ordination - und plötzlich wird der Bildschirm schwarz! Ein Krypto-Trojaner beginnt, sämtliche (Patienten-)Daten zu verschlüsseln.

Geistesgegenwärtig zieht er den Netzwerkstrecker und kann so einen größeren Schaden vermeiden. „Lediglich" 10 % der Daten werden verschlüsselt, die ein IT-Experte teilweise wieder herstellen kann. Der einlangenden Lösegeldforderung gibt dieser Ordinationsbetreiber somit nicht nach.

Fazit: geringer Datenverlust, überschaubare Kosten, Glück im Unglück.

Fall 2: Heikle Privatpatienten-Daten

In einem anderen Fall ging es um einen sogenannten „Promi-Arzt". Auf dessen Server befanden sich zahlreiche Daten zu sowohl medizinisch indizierten als auch rein kosmetischen Behandlungen seiner Privatpatienten, darunter auch solche, die durchaus in der Öffentlichkeit stehen. Der Server wurde gehackt, die Daten verschlüsselt. Die Erpressung bezog sich hier, ganz bewusst, darauf, dass die Cyber-Verbrecher damit drohten, die Daten der prominenten Patienten ins Netz zu stellen.

Der Betroffene zahlte, erhielt den Krypto-Code und hatte kurz darauf alle seine Daten wieder zugänglich. Die Zahlung erfolgte, wie in fast allen diesen Fällen gefordert, in Bitcoins - freundlicherweise lieferten die Gauner übrigens gleich eine Erläuterung mit, wie diese beschafft und „überwiesen" werden können.

F*azit: „Ehrliche Gauner*", aber wie ist es im nächsten Fall?

Fall 3 - 7: Weitere Datenerpressungsfälle

Ob die Bezahlung des Lösegelds je empfehlenswert ist, darüber streiten sich die Geister … Aber dieser Fall und ähnliche sind auch aus anderen Gründen interessant: Einmal wird klar, dass es auch gezielte Hacks gibt; und einmal haben wir gelernt, dass beim Erpressungsgeld absolut Unterschiede der Höhe nach gemacht werden. Einmal sollten es € 2.000,- und € 3.000,- sein, damit die Daten nicht an die Öffentlichkeit gelangten; hier € 5.000,- und in einem besonders heiklen Fall waren sogar € 50.000,- gefordert!

Die Mehrzahl unserer Klienten hat übrigens *nicht* bezahlt und Spezial-IT-Unternehmen beauftragt, den Kryptocode zu entschlüsseln und den Datenzugriff wiederherzustellen.

Mit unterschiedlichem Erfolg, aber grundsätzlich scheint die Wiederherstellung durchaus möglich. Kostenpunkt jeweils ab € 2.000,- und bis zu € 10.000,-.

Diese Datenwiederherstellungskosten sind grundsätzlich gut in modernen Cyber-Versicherungen absicherbar (siehe Artikel-Teil 18 aus ÖZZ 6/2017 zu den aktuell verfügbaren Versicherungslösungen). Die speziell angesprochene Gefahr der Datenveröffentlichung geht aber natürlich auch Hand in Hand mit der Sorge vor Vertrauensverlust sowie mit dem naheliegenden Vorwurf dieser Patienten, man habe deren Daten nicht ausreichend geschützt. Hier kommt dann die Haftpflichtversicherung zum Tragen. Vielleicht auch interessant: die Hardware selbst war nur in einem uns bekannten Fall tatsächlich unbrauchbar beschädigt und musste getauscht werden, Kostenpunkt € 1.500,- (die in einer speziellen Geräteversicherung Deckung fanden).

Fall 8ff: Buttersäureangriff

Auch wenn nicht alles Kriminelles, was per E-Mail ins Postfach flattert, auch wirklich ein Cyber-Verbrechen ist, seien hier auch die aktuellen Erpresser-E-Mails mit der Androhung von Buttersäureangriffen auf Ordinationen erwähnt. Mehrere Zahnärzte sind betroffen und Empfänger solcher E-Mails.

Darin bedroht der Verfasser in, laut Polizeiaussagen, „Rotlichmilieu-Stil" die Ordination mit einem Buttersäureangriff, wenn nicht € 3.000,- in Bitcoins bezahlt würden. Klassische Schutzgelderpressung also. Solche Verbrechenspraktiken dürften sich jetzt auch auf kleine und mittlere Unternehmen, und eben auch Arzt- und Zahnarztpraxen, ausweiten.

Es wird empfohlen, so auch Landes-Zahnärztekammern in aktuellen Rundschreiben, in solchen Fällen die Polizei zu informieren und nicht zu bezahlen.

Versicherungsseitig ist die Drohung mit dem Buttersäureangriff schwierig: Cyberprodukte bieten hier keinen Schutz, denn es geht ja um (angedrohte) physische Angriffe. Wenn dann aber die Ordination selbst gar nicht angegriffen wird, sondern zum Beispiel der Eingangsbereich, dann kommt allerdings auch nicht der üblicherweise vorhandene Vandalismusschutz nach Einbruch zum Tragen. Ein schwierig zu handhabendes Risiko, weil ja auch niemand noch von Fällen weiß, in denen die Drohung auch in die Tat umgesetzt wurde, also wie solche Taten ausgeführt würden.

Wie sich schützen?

Die bittere Wahrheit vorweg: Vollumfassenden Schutz gibt es nicht. Aber: Die Hände in den Schoß legen und sich ohnmächtig fühlen angesichts der neuen Bedrohungsszenarien ist jedenfalls auch nicht hilfreich. Wir genießen die Vorteile des Internet, und wir werden lernen müssen, mit seinen Gefahren zu leben.

Und erste Maßnahmen sind nicht allzu schwer: Wer seine IT überdurchschnittlich sichert, das Virenprogramm am neuesten Stand hält, seine Daten sichert, nicht jedes Attachment öffnet und auch seine Mitarbeiter diesbezüglich schult, die Firewall in Schuss hält und die Passwörter nicht gerade auf seiner Arzttafel notiert, hat bereits gute Chancen, dass der „next door"-Effekt eintritt: die Cyberkriminellen suchen sich ein anderes Opfer, bei dem es noch leichter ist, an interessante Daten zu kommen. Das klingt vielleicht nach einem ungewöhnlichen Rat, aber wer wie wir Versicherungsmakler mit Einbruchsfällen beschäftigt ist, kennt diesen Effekt.

Natürlich ist das nur eine Reduktionsmaßnahme für Ihr Risiko, von Cyberkriminalität selbst betroffen zu sein. Wenn es jemand auf Ihre Daten oder Ihren Schaden abgesehen hat, hilft das natürlich wenig. Für solche Fälle sollten Schäden an Ihrer IT und Datenverlust im regelmäßigen Risk Mapping mit Ihrem Versicherungsberater klar angesprochen werden: Was sind die existenzrelevanten Risiken, gegen die eine zusätzliche Versicherung erforderlich sein könnte? Für diese Risiken kann es dann sinnvoll sein, Ihren Einbruch-Versicherungsschutz um Fälle des „Cyber-Einbruchs" zu erweitern.

Mag. Marcel Mittendorfer
VERAG Versicherungsmakler GmbH
1190 Wien, Eroicagasse 9
www.verag.at