

Wenn die Praxis plötzlich offline ist. Bericht eines echten Cyber-Schadenfalls.

In der Theorie wissen viele Praxisinhaberinnen und -inhaber, dass ein Cyberangriff jederzeit passieren kann. Trotzdem glauben viele, dass eher andere Unternehmen gefährdet sind und hoffen, selbst nicht betroffen zu sein. Was aber, wenn plötzlich die eigene Praxis angegriffen wird? Genau das erlebte eine Arztpraxis, die trotz getroffener Sicherheitsmassnahmen Opfer eines Ransomware-Angriffs wurde. Wir haben mit der verantwortlichen Versicherungsgesellschaft über diesen Fall gesprochen und zeigen, wie eine Cyberversicherung im Ernstfall helfen kann.



Am späten Nachmittag bemerkte zunächst niemand, dass sich Cyberkriminelle Zugriff auf zentrale Serverkonfigurationen der Praxis verschafft hatten. Erst am nächsten Morgen wurde klar, dass wesentliche Systemdateien, welche zum Starten und Laden der Server benötigt wurden, verschlüsselt worden waren. Es handelte sich um einen klassischen Ransomware-Angriff: Die Kriminellen hinterliessen eine sogenannte «Ransomnote», also eine digitale Erpressungsnachricht mit der Aufforderung zur Kontaktaufnahme. Eine konkrete Lösegeldforderung war darin nicht enthalten. Das Ziel der Täter war jedoch klar: Verhandlung und Zahlung.

Betrieb unter Druck – aber keine Patientendaten betroffen

Trotz der Umstände konnte man den Praxisbetrieb aufrechterhalten, der IT-Betrieb war jedoch eingeschränkt. So konnten beispielsweise die behandelnden Ärztinnen und Ärzte ihre Sprechstunden erst im Nachgang dokumentieren und im EDV-System erfassen. Auch die organisatorische und technische Bewältigung der Situation stellte einen Mehraufwand dar. Insgesamt belief sich der zusätzliche interne Aufwand der Praxis auf rund 60 Stunden. Glücklicherweise waren Patientendaten nicht von der Verschlüsselung betroffen. Auch ein Datenabfluss konnte nicht nachgewiesen werden. Die Analysen der IT-Forensik zeigten anhand der Zugriffszeiten, dass ein umfassender Diebstahl der Gesundheitsdaten sehr unwahrscheinlich ist.

Schnelle Hilfe durch Versicherung und Spezialisten

Nach Bekanntwerden des Angriffs handelte die Praxis umgehend und informierte ihren IT-Dienstleister. Gleichzeitig wurde die Cyberversicherung kontaktiert, welche sofort reagierte und innerhalb kürzester Zeit einen spezialisierten IT-Security-Experten für Incident Response und Forensik zur Verfügung stellte. Dieser unterstützte die Praxis bei der technischen Analyse, half beim geordneten Wiederaufbau der Systeme und gab Empfehlungen zur Erhöhung der IT-Sicherheit. Auch juristische Unterstützung wurde organisiert: Ein auf Datenschutzrecht spezialisierter Anwalt half bei der Klärung von Meldepflichten.

Auf eine Kommunikation und Verhandlung mit den Erpressern wurde verzichtet, da die IT-Spezialisten eine Wiederherstellung der EDV-Umgebung innert nützlicher Frist bewerkstelligen konnten. Dank des koordinierten Zusammenspiels aller Beteiligten konnte die IT-Einschränkung auf zwei Tage begrenzt werden. Während dieser Zeit war der Praxisbetrieb zwar erschwert, aber nicht vollständig lahmgelegt und Patienten konnten weiterhin behandelt werden.

Kostenübernahme durch die Cyberversicherung

Der finanzielle Schaden belief sich insgesamt auf rund 25 000 Franken. Der grösste Teil entfiel auf die verschiedenen IT-Arbeiten, welche rund 18 000 Franken gekostet haben. Hinzu kamen interne Mehrkosten von rund 5 000 Franken sowie juristische Beratungskosten von etwa 2 000 Franken. Nach Abzug des Selbstbehalts übernahm die Versicherung sämtliche Kosten. Der finanzielle Schaden für die Praxis beschränkte sich dank der Cyberversicherung somit auf den Selbstbehalt.

Fazit

Dieser Fall zeigt eindrücklich, wie schnell eine Praxis in eine ernste Lage geraten kann und wie wertvoll die Unterstützung durch spezialisierte Partner ist. Während in der Öffentlichkeit oft nur über Grossangriffe berichtet wird, sind es in der Realität häufig

kleinere und mittelgrosse Unternehmen wie Arztpraxen, die betroffen sind. Umso wichtiger ist es, gut vorbereitet zu sein, sei es durch technische Sicherheitsmassnahmen, klare Abläufe im Ernstfall und auch eine Versicherung, die im Schadenfall nicht nur zahlt, sondern aktiv unterstützt.

Ist Ihre Praxis ausreichend geschützt?

Cyberangriffe können jede Praxis treffen – auch mit bestehenden sorgfältigen Sicherheitsmassnahmen. Wir beraten Sie gerne persönlich und erstellen Ihnen eine unverbindliche Offerte – kostenlos und auf Ihre individuelle Situation abgestimmt. Rufen Sie uns unter 031 959 50 00 an oder besuchen Sie unsere Website unter www.fmhinsurance.ch/cyber.

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

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