Ransomware

Sind Lösegeldzahlungen tabu?

Behörden raten von Lösegeldzahlungen bei Ransomware-Attacken ab. Für betroffene Unternehmen können solche Zahlungen jedoch manchmal das einzig verbleibende und vertretbare Mittel zur Wiedererlangung verschlüsselter Daten sein.

→ VON ROLAND MATHYS

Roland Mathys
Der Rechtsanwalt und Wirtschaftsinformatiker leitet als Partner das Technologie-, Daten- und Cyberrechtsteam von Schellenberg Wittmer Rechtsanwälte in Zürich und ist Co-Leiter der Rechtskommission von swissICT.

Wird ein Unternehmen Opfer einer Ransomware-Attacke, folgt meist eine Lösegeldforderung der Cyberkriminellen. Für das betroffene Unternehmen stellt sich dann die Frage, ob auf eine solche Forderung zur Wiederherstellung verschlüsselter Daten überhaupt eingegangen werden soll.

Von der Zahlung von Lösegeld wird seitens Straf- und Untersuchungsbehörden, aber auch durch das BACS mit Nachdruck abgeraten. Denn: Mit dem Erhalt von Lösegeld erreichen die Hacker ihr Ziel, was verhindert werden muss. Zudem wird dadurch der Kreislauf der Wirtschaftskriminalität finanziert und am Leben erhalten.

Dem ist nicht grundsätzlich zu widersprechen. Dennoch bleibt offen, wie ein betroffenes Unternehmen mit diesem Dogma umgehen soll: Sind Lösegeldzahlungen in jedem Fall ein Tabu? Also auch dann, wenn dies als einziger Ausweg bleibt, um innert nützlicher Frist wieder an geschäftskritische verschlüsselte Daten zu gelangen?

LÖSEGELDZAHLUNG ALS OPTION?

Bei einer erfolgreichen Cyberattacke muss ein Unternehmen alle Optionen prüfen, um Schaden vom Unternehmen abzuwenden oder möglichst zu minimieren. Steht kein Backup der verschlüsselten Daten zur Verfügung und können die betroffenen Daten nicht anderweitig entschlüsselt oder wiederhergestellt werden, muss aus unternehmerischer Sicht auch die Zahlung von Lösegeld als Möglichkeit zur Wiedererlangung der Daten in Betracht gezogen werden – jedenfalls dann, wenn es sich um geschäftskritische Daten handelt und das Risiko existenzbedrohender Betriebsausfälle droht.

«Bei einer erfolgreichen Cyberattacke muss ein Unternehmen alle Optionen prüfen.»

Roland Mathys
Co-Leiter Rechtskommission swissICT

Dies soll kein Plädoyer für Lösegeldzahlungen sein! Stereotype behördliche Ablehnung und Stigmatisierung solcher Zahlungen helfen einem betroffenen Unternehmen jedoch nicht weiter. Vielmehr muss sich das Unternehmen fragen, ob Lösegeldzahlungen rechtlich zulässig sind und wann sie im Einzelfall unter Abwägung aller auf dem Spiel stehender Güter eine Option darstellen können.

SIND LÖSEGELDZAHLUNGEN VERBOTEN?

Die Zulässigkeit von Lösegeldzahlungen wird international nicht einheitlich beurteilt. In der Schweiz sind Lösegeldzahlungen meist nicht strafbar. In einem solchen Fall liegt keine Geldwäscherei vor und

«Die Zahlung von Lösegeld bei einem Ransomware-Angriff soll wenn immer möglich vermieden werden.»

Roland Mathys
Co-Leiter Rechtskommission swissICT

eine mit der Zahlung allfällig verbundene Unterstützung einer kriminellen Organisation lässt sich mit Notstand rechtfertigen.

Vorsicht ist dort geboten, wo konkrete Hinweise bestehen, dass die Erpresser einem sanktionierten Personenkreis angehören oder dass die Zahlungen einer sanktionierten Institution oder einem mit einem Embargo belegten Staat zu Gute kommen.

Lösegeldzahlungen an sanktionierten Personenkreise, Institutionen oder Staaten können auch in der Schweiz strafbar sein.

WANN KANN EINE LÖSEGELDZAHLUNG SINN MACHEN?

Wird von der Zulässigkeit ausgegangen, stellt sich die Frage, in welchen Situationen eine Lösegeldzahlung ein taugliches Mittel zur Wiedererlangung der Daten darstellen kann. Dabei sind verschiedene Kriterien zu berücksichtigen:

- Eine Lösegeldzahlung kann dort angebracht sein, wo Daten «nur» verschlüsselt und nicht auch exfiltriert wurden. Im letzteren Fall bleibt nämlich die Gefahr bestehen, dass die Kriminellen trotz Lösegeldzahlung die Drohung aufrechterhalten, die gestohlenen Daten im Darkweb zu publizieren, um damit weitere Zahlungen zu erpressen.
- Auch im Falle einer Zahlung ist keineswegs garantiert, dass die Erpresser den Schlüssel effektiv herausgeben werden. Deswegen sollte man sich vorgängig über einschlägige Quellen ein Bild über die «Seriosität» der fraglichen Erpresser(-bande) verschaffen. Ist ihre Reputation schlecht, lohnt sich eine Zahlung kaum, da die Cyberkriminellen unwillig (oder technisch nicht in der Lage) sind, den Schlüssel in einer brauchbaren Form zu liefern.
- Bei gewissen Cyberversicherungen sind Lösegeldzahlungen (meist begrenzt auf eine bestimmte Summe) in der Deckung eingeschlossen, was den Entscheid zur Zahlung erleichtern kann. Es lohnt sich daher, die Versicherungsdeckung im Vorfeld genau zu klären.
- Pflichten zur behördlichen Meldung von Data Breaches oder Cybervorfällen können durch die Zahlung von Lösegeld meist nicht abgewendet werden, auch wenn die betroffenen Daten nur für kurze Zeit nicht verfügbar sind. Soll also eine Ransomware-Attacke vertraulich bleiben, hilft die Lösegeldzahlung wenig. Im Gegenteil kann die Lösegeldforderung erhöhte Publizität auslösen: Beispielsweise müssen Lösegeldzahlungen als ausserordentlicher Aufwand im Anhang zur Jahresrechnung offengelegt werden. In der Schweiz wird zudem die Einführung einer Pflicht diskutiert, Lösegeldzahlungen den Behörden zu melden.

PRAKTISCHE TIPPS

Erwägt ein Unternehmen die Zahlung von Lösegeld, empfiehlt sich der Beizug spezialisierter Verhandler, die versuchen, die Forderung möglichst zu reduzieren und dabei auch nützliche Informationen über die Erpresser zu gewinnen (z.B. Zugehörigkeit zu einer Bande, Herkunft, Verlässlichkeit).

Auch kann die Involvierung der Strafbehörden sinnvoll sein. Etwa um eine Lösegeldzahlung in Kryptowährung nachzuverfolgen und damit möglicherweise die Täter aufzuspüren. Ein vorgängiges informelles Gespräch mit Strafverfolgungsbehörden kann zudem Aufschluss über den (nach unseren Erfahrungen meist geringen) behördlichen «Appetit» geben, die Zahler von Lösegeld strafrechtlich zu belangen und damit die Opfer zu Tätern zu machen.

Vor Leistung der Lösegeldzahlung sollte die Tauglichkeit und Funktionsfähigkeit des Schlüssels an einem Teil der betroffenen Daten getestet werden. Bieten die Erpresser keinen Test an oder scheitert dieser, ist dies meist ein starkes Indiz, von der Zahlung abzusehen.

Fazit: Die Zahlung von Lösegeld bei einem Ransomware-Angriff soll wenn immer möglich vermieden werden. Fehlen wirksame Alternativen und sind die Erfolgsaussichten intakt, sollte sie als ultima ratio jedoch in die Erwägungen einbezogen statt kategorisch stigmatisiert werden. ←

Rechtskommission swissICT:

Die Autor:innen bringen ihr Fachwissen aktiv in die Rechtskommission des Verbands swissICT ein. Mit viel Engagement gestalten sie die Branche mit und sensibilisieren Anbieter:innen und Nutzer:innen von IT-Leistungen für relevante juristische Fragestellungen auf politischem Parkett, bei Fachveranstaltungen und in Verbandsprojekten.
→ **www.swissict.ch**