Erfolgreiches Management bei Cybercrime Attacken

In der heutigen digitalisierten Geschäftswelt kommt persönlichen Daten der Kundinnen und Kunden ein grosser Wert zu. Entsprechend werden auch Angriffe auf Netzwerke, Server und Datenbanken häufiger. Die Kanzlei Burkhalter Rechtsanwälte unterstützte kürzlich eine Klientin beim Management einer Cybercrime Attacke. Im Folgenden zeigt das Legal Team unter der Leitung von Rechtsanwalt Dr. iur. Matthias Amgwerd die juristischen Schritte auf, die sie zur Wahrung der Sorgfaltspflichten unternommen haben.

Informationspflichten gegenüber den Kunden

Selbstverständlich müssen in einem allerersten Schritt alle technischen Massnahmen ergriffen werden, um das Datenleck zu schliessen und sämtliche Daten zu sichern. Diese Schadenminderungspflicht übergibt man indes vorzugsweise dem Informatikspezialisten und nicht dem Rechtsanwalt. Im Falle einer Cyberattacke, bei der Kundendaten betroffen sind, hat man dann sogleich die Informationspflichten gegenüber den Kundinnen und Kunden zu erfüllen. Gestützt auf das geltende schweizerische Datenschutzgesetz (DSG, SR 235.1) besteht zumindest keine explizite Informationspflicht. Vielmehr ergibt sich diese aus den allgemeinen Sorgfaltspflichten gemäss dem jeweiligen Vertrag, der zwischen dem betroffenen Unternehmen und seinen Kunden besteht. Im Anwendungsbereich der Europäischen Datenschutzgrundverordnung (DSGVO) besteht gemäss Art. 34 Abs. 1 DSGVO die Verpflichtung, die von einer Datenschutzverletzung betroffenen Personen unverzüglich zu benachrichtigen, wenn diese ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge hat.

Meldepflichten gegenüber den Behörden

In einem weiteren Schritt sollte der Vorfall so bald als möglich den zuständigen Behörden gemeldet werden. In der Schweiz empfiehlt sich eine Meldung beim Eidgenössischen Datenschutzbeauftragten (EDOEB), beim Bundesamt für Polizei (fedpol) sowie bei der Melde- und Analysestelle für Informationssicherheit (MELANI). Gemäss Art. 33 DSGVO ist die Datenschutzverletzung binnen 72 Stunden seit Bekanntwerden des Vorfalles der zuständigen nationalen Aufsichtsbehörde zu melden.

Strafrechtliches Vorgehen

Des Weiteren sollte eine Strafanzeige in Betracht gezogen werden. Allerdings stellt sich bei Cyber-Delikten oft die Frage nach der örtlichen Zuständigkeit. Zudem ist die Täterschaft oft unbekannt. Gemäss Art. 426 Abs. 2 StPO (SR 312.0) können die Verfahrenskosten indes der Privatklägerschaft auferlegt werden, wenn das Verfahren eingestellt oder die beschuldigte Person freigesprochen wird. Insofern ist abzuwägen, welche Anträge man im Rahmen der Strafanzeige stellen will und ob allenfalls eine „stumpfe“ Strafanzeige ohne Konstituierung als Privatklägerschaft das Mittel der Wahl ist. Das strafrechtliche Vorgehen birgt eine gewisse Tücke: Falls sich im Rahmen der Ermittlungen zeigt, dass das betroffene Unternehmen den Angriff mitverschuldete, weil es die Daten nicht ausreichend schützte (eine entsprechende Pflicht besteht

auch nach DSG [Art. 7] und DSGVO [Art. 32]), kann unter Umständen dessen Organen vorgeworfen werden, dass sie das Datendelikt durch unverantwortliches Handeln ermöglicht haben. Diesfalls riskieren sie in zivilrechtlicher Hinsicht eine Organhaftung und können sich in strafrechtlicher Hinsicht der ungetreuen Geschäftsbesorgung (Art. 158 StGB, SR 311.0) strafbar machen. Der Vorwurf trifft ausserdem zunächst das Unternehmen selbst (Art. 102 StGB).

Zivilrechtliches Vorgehen

Liegen Ergebnisse einer strafrechtlichen Untersuchung vor oder sind sonstige greifbare Beweise vorhanden, lohnt es sich, unter Umständen eine Zivilklage in Betracht zu ziehen. Die Zivilklage kann sich gegen die Täterschaft aus Deliktshaftung stützen, sie kann aber auch gegen einen allfälligen fehlbaren Vertragspartner aus einer Vertragsverletzung geltend gemacht werden. Sofern ein zivilrechtliches Vorgehen gewünscht ist, ist zunächst einmal der Ausgang des Strafverfahrens abzuwarten. Ausserdem ist auf eine detaillierte und umfassende Dokumentation zu achten, damit ein Schaden bewiesen werden kann. Allerdings birgt eine Zivilklage gewisse Risiken, gerade auch in finanzieller Hinsicht (Verfahrens- und Anwaltskosten).

In jedem Fall: Beizug von Experten

Eindrücklich zeigte sich am eingangs erwähnten Fall, dass der sofortige Beizug eines Expertenteams unerlässlich ist. Betroffene Unternehmen sollten nicht nur Informatik- und Technikspezialisten, sondern auch (Datenschutz-)Rechtsexperten beiziehen. Nicht zuletzt ist eine sorgfältige Kommunikation und eine vorausschauende Planung, gerade auch um allfällige Schadenersatzansprüche geltend zu machen, gefordert.

Rechtsanwalt Dr. iur. Matthias Amgwerd und Legal Team, Burkhalter Rechtsanwälte