Mit Cyberattacken ist zu rechnen

Anwaltskanzleien · Am besten schützt man sich vor Angriffen auf Computersysteme mit sicheren Systemen und Backups. Im Ernstfall ist für Kanzleien zentral: Das Anwaltsgeheimnis muss gewahrt werden.

DLA PIPER / DIC ASSET

Die Digitalisierung des Berufsalltags bietet der Anwaltschaft viele Chancen – sie birgt aber auch beträchtliche Risiken. Anwaltskanzleien verfügen über grosse Mengen an vertraulichen und oft höchst sensiblen Daten. Deshalb sind sie attraktive Ziele für Cyberkriminelle. Während bei kleineren Kanzleien das Thema Cybersicherheit – wohl oft aus Kostengründen – noch stiefmütterlich behandelt wird, beschäftigen grössere Sozietäten eigene Abteilungen für Informationstechnologie (IT). Dennoch schützt hoher IT-Aufwand nicht vor schwerwiegenden Vorfällen.

> “Bereits Minuten können einen massgeblichen Unterschied im Schadenausmass bedeuten”

Publik wurde etwa die Cyberattacke auf DLA Piper, eine in 40 Ländern vertretene Anwaltskanzlei. Eine Variante des Kryptotrojaners Petya verschlüsselte nicht nur bestimmte Dateien auf den betroffenen Rechnern, sondern befiel kritische Bereiche der primären Festplatte und verhinderte damit den Start des Betriebssystems. Berichten zufolge war die weltweite IT-Infrastruktur der Kanzlei über mehrere Tage nicht verfügbar. Die anonyme Urheberschaft forderte eine Lösegeldsumme in Bitcoins. Viele andere Cyberattacken werden gar nicht erst publik. Über die Dunkelziffer kann man nur spekulieren – auch in der Schweiz.

Cyberangriffe sind aus verschiedenen Gründen gefährlich. Einerseits stellen sie ein operationelles Risiko dar, zumal bei Ausfall der IT eine Anwaltskanzlei beinahe stillsteht. Unter anderem droht der Verlust von Daten, das Verpassen von Fristen – der typische Fall der anwaltlichen Sorgfaltspflichtverletzung – sowie ein enormer Reputationsschaden. Grosse Teile der gespeicherten Daten sind zudem vom Anwaltsgeheimnis (Artikel 13 Anwaltsgesetz, BGFA) geschützt, dessen Verletzung gemäss Strafgesetzbuch (Artikel 321 StGB) strafbar ist.

Standards für präventive Massnahmen

Weder Gesetz noch Standesrecht schreiben der Anwaltschaft bestimmte Massnahmen zur Herstellung einer adäquaten IT-Sicherheit vor. Doch ist aufgrund der anwaltlichen Sorgfaltspflicht (Artikel 12 BGFA) und des Datenschutzgesetzes (DSG) ein Mindestmass an Sicherheit zu erwarten. Als Orientierungspunkt für die organisatorischen und technischen Vorkehrungen dienen international anerkannte Standards wie das Cybersecurity-Framework des National Institute of Standards and Technology (NIST). Ursprünglich war es zum Schutz kritischer Infrastrukturen (wie etwa der Energieversorgung und der Telekommunikation) entwickelt worden, wurde aber auch rasch in weiteren Kreisen zum gängigen Standard im Umgang mit Cyberrisiken.

Der mehrstufige Aufbau mit den fünf Funktionen Identify, Protect, Detect, Respond und Recover ist umfassend und trotzdem leicht verständlich. In organisatorischer Hinsicht sind klare Entscheidungsprozesse und interne Verantwortlichkeiten zu definieren, damit im Ernstfall rasch und entschieden reagiert werden kann. Fehlt es intern am technischen Know-how, ist der Beizug von externen Fachleuten angezeigt. Die sich im Ernstfall stellenden Fragen (Wer ist zu informieren? Wer entscheidet? Wie ist intern und gegenüber Kunden zu informieren? Bestehen Meldepflichten?) müssen vorgängig diskutiert und sorgfältig abgeklärt werden. Zu prüfen ist allenfalls der Abschluss einer speziellen Cyberversicherung, die auch Kosten des Krisenmanagements decken kann. Dabei sind die Ausschlüsse und Haftungslimiten zu beachten.

Die Cloud als heikler Datenspeicher

Eine weitere Herausforderung birgt das zunehmende Verwenden von Cloud-Lösungen. Zwar ermöglichen diese erhebliche Effizienzgewinne. Einige rechtlich heikle Punkte sind jedoch zu beachten. Die meisten Anbieter von Cloud-Diensten sind US-amerikanische Unternehmen (Amazon, Microsoft, Google, Dropbox etc.). Ihnen zugänglich gemachte Daten gelangen dadurch in den Einflussbereich von US-Behörden.

DLA Piper in Frankfurt: Die internationale Kanzlei – hier in den obersten sieben Etagen – wurde Opfer von Erpressern

Dieses Risiko hat sich infolge des 2018 erlassenen Cloud Acts weiter verschärft. Aus Sicht der Anwaltskanzlei lässt sich bei gängigen Cloud-Lösungen kaum sicherstellen, dass die entsprechenden Daten ausschliesslich auf Servern in der Schweiz gespeichert oder verarbeitet werden. Dies ist vor dem Hintergrund der in der Praxis wichtigen Artikel 271 StGB (verbotene Handlungen für einen fremden Staat) und 273 StGB (wirtschaftlicher Nachrichtendienst) problematisch. Schliesslich ist das Anwaltsgeheimnis zu berücksichtigen. Verschlüsselt eine Kanzlei die Daten vor der Übertragung an den Provider und verfügt dieser nicht über den Schlüssel, liegt wohl kein Offenbaren von Geheimnissen im Sinne von Artikel 321 StGB vor. Im Einzelfall ist zu prüfen, wie dies praktisch umgesetzt werden kann, wobei je nach Cloud-Provider Unterschiede bestehen.

Wenn eine Cyberattacke erkannt wird – dies kann je nachdem erst Monate nach dem Beginn des Angriffs geschehen –, ist rasches Handeln gefragt. Bei Cyberattacken können bereits Minuten einen massgeblichen Unterschied im Schadenausmass bedeuten. Umgehend sind die notwendigen Schritte gemäss dem vorgängig festgelegten Prozess einzuleiten. Nach einem Cyberangriff gilt es, das volle Ausmass der Sicherheitsverletzung festzustellen. Nur so lässt sich eruieren, wie und wo die Täter in die Systeme eindrangen und welche Daten sie allenfalls stahlen oder manipulierten.

Nach einer Cyberattacke Beweise sichern

Angegriffene IT-Systeme sind als Tatorte zu behandeln. Unkoordinierte Handlungen führen dazu, dass Spuren verändert und möglicherweise bedeutende Beweismittel kompromittiert werden. Bei forensischen Untersuchungen geht es nicht in erster Linie darum, die Täter zu ermitteln, sondern die Vorgehensweise nachzuvollziehen und dabei mögliche Beweise zu sichern. Ein Angriff sollte trotz sorgfältiger Bearbeitung nicht als abgewendet betrachtet werden, bis die fachgerechte Ursachenanalyse abgeschlossen ist. Zudem stellt sich die Frage der Meldung eines Cybervorfalles.

Im Gegensatz zum Finanzsektor und anderen als kritische Infrastrukturen geltenden Sektoren haben Anwälte heute keine spezifische gesetzliche Meldepflicht. Freiwillig können Vorfälle bei der Melde- und Analysestelle Informationssicherung des Bundes (Melani) gemeldet werden. Diese kann jedoch in der Regel keine Unterstützung bei der Bewältigung bieten. Zu prüfen ist im Einzelfall eine mögliche Meldepflicht gemäss der EU-Datenschutz-Grundverordnung (DSGVO) beziehungsweise in naher Zukunft nach dem revidierten Schweizer Datenschutzgesetz. Zu prüfen wird auch sein, ob Schadenmeldungen an Versicherungen zu tätigen sind.

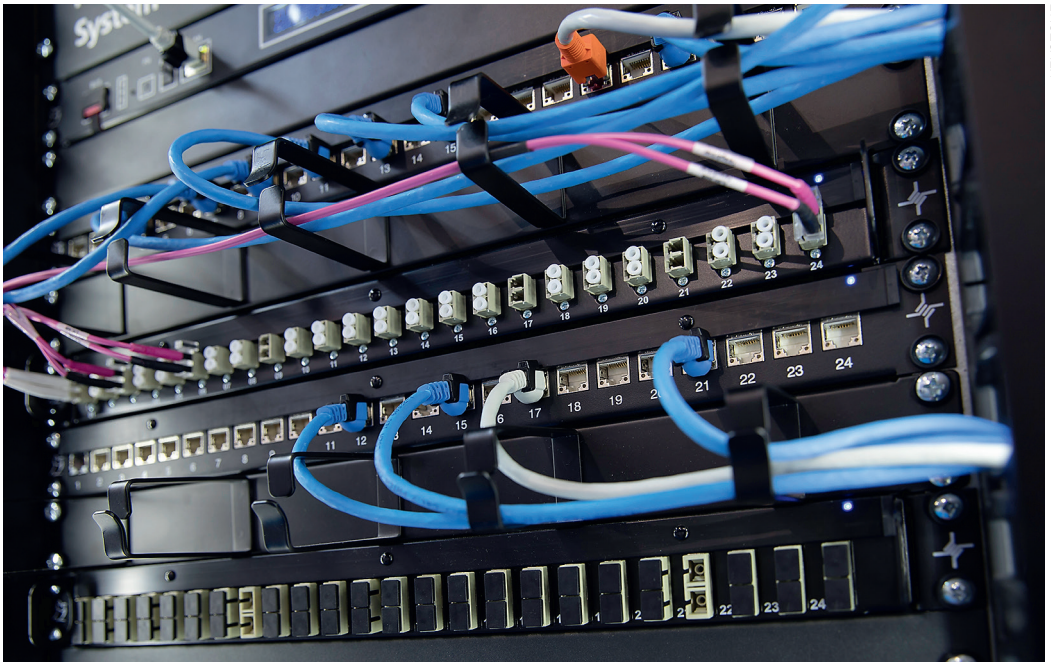
Grundsätzlich besteht bei einem Angriff die Möglichkeit einer Strafanzeige. In mehreren Kantonen existieren spezialisierte Cyber-Strafverfolgungskapazitäten. Wird eine Anzeige erwogen, ist

sie sinnvollerweise rasch einzureichen. Allerdings stellt das Anwaltsgeheimnis – neben Reputationsbedenken – für das Einreichen einer Strafanzeige eine besondere Hürde dar.

Anwälte und ihre Hilfspersonen unterstehen zeitlich unbegrenzt und gegenüber jedermann dem Berufsgeheimnis über alles, was ihnen infolge ihres Berufes von ihrer Klientschaft anvertraut wurde (Artikel 13 BGFA). Nicht strafbar ist die Offenbarung im Falle der Einwilligung durch die Klientschaft oder der Entbindung durch die kantonale Aufsichtsbehörde (Artikel 321 Absatz 2 StGB). Die Bekanntgabe geschützter Daten an Strafverfolgungsbehörden ist somit grundsätzlich nicht zulässig.

Da die Möglichkeit der Kenntnisnahme genügt, müsste eine Behörde solche Daten im Rahmen der Ermittlung nicht einmal tatsächlich eingesehen haben, damit das Anwaltsgeheimnis als verletzt gälte, sondern lediglich den Zugang dazu erhalten. Einfachere Fälle ausgenommen, wird die Ermittlungsbehörde jedoch wohl Zugang zur vom Cyberangriff betroffenen Infrastruktur und somit den sich darauf befindenden Daten benötigen.

Falls aus Ermittlungsgründen zeitliche Dringlichkeit besteht, wird die Entbindung vom Anwaltsgeheimnis – gerade bei einer Vielzahl von Klienten – kaum innert nützlicher Frist realisierbar sein. Ebenso zeitaufwendig ist eine Entbindung durch die Aufsichtskommission, die zudem nur dann erfolgen kann, wenn das Interesse der Kanzlei an der Strafverfolgung deutlich höher gewichtet wird als das Interesse der Klientschaft an der Geheimhaltung (siehe etwa § 34 Absatz 3 Anwaltsgesetz des Kantons Zürich) – was bei Cyberangriffen nicht ohne Weiteres anzunehmen ist. Eine manuelle Triage aller Daten und nachfolgende Aussonderung der vom Anwaltsgeheimnis geschützten Daten, wie sie etwa bei der strafprozessualen Siegelung geschieht, fällt sodann schon aus Praktikabilitätsgründen ebenfalls ausser Betracht. Die Prüfung aller Datensätze würde Wochen bis Monate dauern. Ebenso wenig denkbar sind technische Vorkehrungen, um den unbefugten Zugriff auf vom Anwaltsgeheimnis geschützte Daten zu verhindern. Der Schutz des Anwaltsgeheimnisses dürfte somit in vielen Fällen den Beizug der Strafverfolgungsbehörden ausschliessen.



KEYSTONE

Bei Cyberangriff rasch handeln: Jede Minute zählt

Informelle Vorgespräche mit der Staatsanwaltschaft

Das heisst jedoch nicht, dass eine Strafanzeige in jedem Fall von vornherein ausgeschlossen ist. Unter Umständen können die Strafverfolgungsbehörden auch ohne Zugang auf vom Anwaltsgeheimnis geschützte Daten Ermittlungen anstellen. Ob dies im konkreten Fall möglich ist, kann im Rahmen eines informellen Vorgesprächs mit der Staatsanwaltschaft eruiert werden. Ein solches Gespräch kann erste Anhaltspunkte geben, welche Daten gebraucht werden. Allenfalls fallen dabei nur Protokolldateien (Logfiles) in Betracht, welche keine geschützten Informationen enthalten.

Empfehlenswert ist jedoch in vielen Fällen der Beizug eines spezialisierten IT-Dienstleisters. Dieser kann als Hilfsperson vertraglich in den Kreis der Träger des Anwaltsgeheimnisses eingebunden werden. Eine vergleichbare Vereinbarung mit einer Strafverfolgungsbehörde, worin diese ihre Verschwiegenheit zusichert, wäre nach unserer Meinung hingegen nichtig (vgl. BGE 136 II 415).

Cyberrisiken stellen die Anwaltschaft somit vor eine Vielzahl kniffliger organisatorischer und rechtlicher Fragen. Der Prävention ist ein hoher Stellenwert beizumessen und im Ernstfall muss richtig reagiert werden. Wird eine Strafanzeige erwogen, gilt es, das Anwaltsgeheimnis zu beachten.

Sanija Ameti, Andreas Hösli und Philipp Leo

> **“Der Schutz des Anwaltsgeheimnisses dürfte in vielen Fällen den Beizug der Strafverfolgungsbehörden ausschliessen”**