© Deutscher Apotheker Verlag

Cyberrisiken in der Apotheke

Ansprüche, Haftung und Möglichkeiten der Absicherung

Die wirtschaftlichen Risiken durch sogenannte Cyberangriffe nehmen branchenübergreifend kontinuierlich zu. Spätestens seit im Mai 2017 der Cyberangriff durch die Schadsoftware „Wannacry“ in 150 Ländern u. a. die Systeme von Krankenhäusern, Firmen und staatlichen Institutionen mit Lösegeldforderungen blockierte, sollte jedem klar sein, dass Cyberangriffe ein Massenphänomen geworden sind und ein realistisches Risiko besteht, Opfer eines solchen Angriffs zu werden. Vor Kurzem ist zudem eine Sicherheitslücke bekannt geworden, welche die Hauptprozessoren von Milliarden Computern, Smartphones und Tablets weltweit betrifft und durch die Angreifer an vertrauliche Daten kommen könnten.

Die Erscheinungsformen der Angriffe und Schäden sind vielfältig. Neben digitaler Erpressung mittels „Ransomware“ kann es etwa zu Datendiebstahl, zur Verletzung von Betriebs- und Geschäftsgeheimnissen oder zur Schädigung der eigenen Systeme durch Computerviren kommen. Die meisten Apotheken dürften durch ihre Softwarehäuser vor derartigen Angriffen geschützt sein. Aber was ist, wenn die Schutzsysteme doch einmal versagen? Dieser Beitrag gibt einen Überblick, welche Ansprüche gegen Dritte im Falle eines Angriffs gestellt werden können, welche eigenen Haftungsrisiken bestehen und wie Unternehmen den Gefahren begegnen sollten.

Ansprüche gegen Dritte

– **Angreifer:** Sofern die Identifizierung des Angreifers gelingt, kann dieser auf Schadensersatz in Anspruch genommen werden. Anspruchsgrundlagen sind etwa § 823 Abs. 2 BGB in Verbindung mit verschiedenen strafrechtlichen Normen (u. a. § 303b StGB oder § 17 UWG). Um den Angreifer zu identifizieren, muss regelmäßig dessen IP-Adresse ermittelt werden, wobei die Kosten der Ermittlung als mittelbarer Schaden erstattungsfähig sein können. Allerdings ist diese Ermittlung auch wegen datenschutzrechtlicher Beschränkungen häufig schwierig und erfolglos. Viele Angreifer sitzen zudem im Ausland. Obwohl bei einem Angriff auf deutsche Computer grundsätzlich sowohl deutsches Sachrecht anwendbar ist (Art. 4 Abs. 1 Rom II-VO) als auch ein deutscher Gerichtsstand besteht (Art. 7 Nr. 2 EuGVVO bzw. Art. 6 Abs. 1 EuGVVO i. V. m. § 32 ZPO), gelingt die Durchsetzung von Schadensersatzansprüchen gegen im Ausland sitzende Angreifer in der Praxis nur selten, wenn diese sich dem Verfahren in Deutschland zu entziehen versuchen. Bessere Erfolgsaussichten kann ein Vorgehen gegen einen deutschen Strohmann haben. Gerade bei „Phishing“-Attacken werden manchmal Inhaber von deutschen Bankkonten zwischengeschaltet, die dann den erbeuteten Betrag gegen eine Provision an die Hintermänner weiterleiten. Solche Unterstützer haften regelmäßig für den vollen Schaden und können sich auch nicht darauf berufen, dass das Geld nicht mehr in ihrem Besitz ist (vgl. § 819 BGB). Die Personen, derer sich die Angreifer bedienen, müssen mindestens fahrlässig handeln – etwa wenn sie ohne Mühe die betrügerische Absicht des Hintermannes hätten erkennen können.

– **Banken:** Wenn durch eine Cyberattacke eine nicht autorisierte Überweisung veranlasst wird, haftet die Bank generell nach § 675u Satz 2 BGB. Falls der Bankkunde dem Zahlungsvorgang zugestimmt oder auch nur einen äußerlichen Anschein gesetzt hat, entfällt jedoch die Haftung der Bank.
Dem Anspruch des Bankkunden kann ein aufrechenbarer Gegenanspruch der Bank nach § 675v BGB entgegenstehen, wenn der Bankkunde beispielsweise seine Bank-PIN nicht sicher aufbewahrt hat. Sofern Gegenansprüche der Bank bestehen, kommt deren Kürzung aufgrund Mitverschuldens in Betracht, wenn die Bank ihre Sicherheitssysteme nicht dem aktuellen Stand der Technik angepasst hat.

– **Dienstleister:** Externe Dienstleister haben IT-Sicherheitsbelange des Auftraggebers zu beachten und können sich dabei auf vielfältige Weise schadensersatzpflichtig machen. Besondere Pflichten ergeben sich teilweise durch spezialgesetzliche Regelungen einzelner Segmente. So sind etwa Anbieter von Telemediendiensten nach § 13 Abs. 7 TMG verpflichtet, für geschäftsmäßig angebotene Telemedien sicherzustellen, dass ihre technischen Einrichtungen nach dem Stand der Technik vor unerlaubtem Zugriff geschützt und vor Datenschutzverletzungen sowie Störungen durch äußere Angriffe gesichert sind.

– **Hersteller und Verkäufer von Sicherheitssoftware:** Hersteller und Verkäufer von beispielsweise fehlerhaften Antivirenprogrammen können sowohl vertraglich als auch deliktisch, also zivilrechtlich aufgrund einer unerlaubten Handlung, haften. Im Rahmen der deliktischen Ansprüche ist insbesondere an die Produzentenhaftung aus § 823 Abs. 1 BGB zu denken (im privaten Bereich auch gemäß § 1 Abs. 1 ProdHaftG). Da die Angreifer immer neue Methoden entwickeln, spielen Produktbeobachtungspflichten und nachträgliche Sicherheitsupdates eine wichtige Rolle. Werden Sicherheitslücken bekannt, sind die Softwarehersteller verpflichtet, kurzfristig Sicherheitsupdates zur Verfügung zu stellen. Eine Verletzung dieser Pflicht kann zu Schadensersatzansprüchen führen.

Foto: Gina Sanders – stock.adobe.com

Zugriff verwehren Das ist natürlich das beste Mittel, um Daten zu schützen. Aber hundertprozentigen Schutz gibt es bei keinem Sicherheitssystem. Wer haftet, wenn der Fall der Fälle eintritt und man geschädigt wird?

– **Arbeitnehmer:** Eine besondere Bedeutung kommt Ansprüchen gegen die eigenen Arbeitnehmer zu, da ein erheblicher Teil der Cyberangriffe durch Mitarbeiter erfolgt oder durch diese zumindest begünstigt wird. Bei gezielten Angriffen haften Arbeitnehmer wie externe Angreifer. Wenn aber nur aus Nachlässigkeit etwa eine betriebliche, mit einem Virus infizierte E-Mail geöffnet wird, haften Arbeitnehmer aufgrund des sogenannten Arbeitnehmerprivilegs nur eingeschränkt. Eine volle Haftung kommt dann nur bei grober Fahrlässigkeit und Vorsatz in Betracht.

Eigene Haftung

Wenn es durch einen Cyberangriff zum Zusammenbruch des Betriebssystems kommt, kann dies zu Schadensersatzansprüchen von Kunden führen, denen beispielsweise zugesagte Waren nicht geliefert werden können. Schadensersatzansprüche können auch durch die Verletzung von Nebenpflichten entstehen, etwa wenn Mitarbeiter versehentlich E-Mails mit schadhaften Anhängen weiterleiten oder wenn Vertragspartner durch einen Datendiebstahl zu Schaden kommen. Das Verschulden der eigenen Mitarbeiter oder Dienstleister wird dabei über § 278 BGB dem Apothekeninhaber zugerechnet. Wichtige zu beachtende Schutznormen sind ab Mai der Art. 32 der dann geltenden europäischen Datenschutz-Grundverordnung (DSGVO) bzw. bis dahin der alte § 9 BDSG, welche Unternehmen die Pflicht auferlegen, technische und organisatorische Sicherheitsmaßnahmen zum Schutz von gespeicherten Daten zu treffen. Begünstigt die Nichtbeachtung dieser Verpflichtung beispielsweise einen Hackerangriff, so kann dies zur Schadensersatzpflicht führen. Sind tatsächlich sensible Daten – etwa Angaben zur Medikation oder Bankinformationen – in die Hände von Cyberkriminellen gelangt, so gelten besondere unverzügliche Informationspflichten gegenüber Betroffenen und Aufsichtsbehörden (vgl. Art. 34 DSGVO ab Mai 2018 bzw. § 42a BDSG). Wenn diese Informationspflichten nicht erfüllt werden, drohen neben Schadensersatzansprüchen auch weitere Sanktionen in Form von Anordnungen und Verboten der Aufsichtsbehörden (§ 38 Abs. 5 BDSG) und Bußgeldern (Art. 83 DSGVO) sowie sogar persönliche Strafbarkeit (§ 44 BDSG).

Möglichkeiten der Absicherung

Cyberangriffe können durch geeignete Maßnahmen deutlich erschwert und in ihren Auswirkungen abgeschwächt werden. Dem Thema IT-Sicherheitsmanagement sollte ein hoher Stellenwert eingeräumt und sichergestellt werden, dass Gefahren für die Informationssicherheit oder Bedrohungen des Datenschutzes durch technische Mindeststandards reduziert werden. Hilfestellungen leistet beispielsweise das Bundesamt für Sicherheit in der Informationstechnik mit Analysen und Empfehlungen zu Cybersicherheit und IT-Grundschutz. Es ist zudem regelmäßig sinnvoll, bei der Analyse und Umsetzung von Sicherheitsmaßnahmen sachverständige Beratung hinzuzuziehen.
Im Falle eines Angriffs ist das Krisenmanagement entscheidend. Es kommt dann auf das frühe Erkennen und eine professionelle Reaktion an. Deshalb ist es empfehlenswert – ggf. mit spezialisierter juristischer Beratung –, einen Notfallplan fürs Krisenmanagement zu entwickeln.
Absoluter Schutz ist freilich nicht zu erreichen. Ein großer Teil der verbleibenden Risiken kann jedoch durch spezialisierte Cyberversicherungen gut abgesichert werden. Klassische betriebliche Versicherungen erfassen Cyberrisiken oft nur ansatzweise oder gar nicht. So sind beispielsweise Betriebsunterbrechungen zwar eigentlich von Sachversicherungen abgedeckt, für den Versicherungsschutz wird aber ein versicherter Sachschaden vorausgesetzt, an dem es bei Cyberangriffen fehlt. Die Versicherungsbedingungen der am Markt angebotenen Cybertarife weichen teilweise erheblich voneinander ab. Gute Versicherungslösungen sollten eine Kostenerstattung für Erpressungsgelder, für Datenforensik, für das Krisenmanagement inklusive Benachrichtigung der betroffenen Kunden und für den Aufwand zur Wiederherstellung der Reputation beinhalten. Viele Versicherer setzen über eine „Stand-der-Technik“-Klausel voraus, dass die Computersysteme immer auf dem neuesten Stand der Technik gehalten werden.
In der Praxis führt dies zu zahlreichen Problemen und kann den Versicherungsschutz erheblich einschränken. Daher sollten nur Tarife gewählt werden, die auf eine „Stand-der-Technik“-Klausel verzichten.
Mit dem Abschluss eines Vertrages sollte indes nicht erst gewartet werden, bis der erste Schadensfall eingetreten ist, da dann viele Versicherer eine Annahme aufgrund von Vorschäden ablehnen. |

Jascha Arif, Rechtsanwalt, und Steffen Benecke, Versicherungsmakler, Hamburg

Tipp

Einen Artikel zur Europäischen Datenschutz-Grundverordnung (DSGVO) finden Sie in DAZ 2017, Nr. 50, S. 81 „Was kommt da auf uns zu? Im Mai 2018 tritt die Europäische Datenschutz-Grundverordnung in Kraft“.

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Zustimmung des Verlags!