CYBERVERSICHERUNG

Ransomware-Attacken –

Foto: Ken Schluchtmann, diephotodesigner.de

...die datenschutzrechtlichen Folgen für die Angegriffenen

Durch die voranschreitende Digitalisierung werden immer mehr Daten in elektronischer Form abgespeichert. Dadurch werden viele Arbeitsprozesse einfacher und effizienter. Allerdings resultiert daraus auch, dass auf besonders schützenswerte persönliche Daten einfacher von unberechtigten Dritten zugegriffen werden kann. Insbesondere aufgrund der erheblichen Zunahme von Ransomware-Attacken seit Beginn der Coronakrise[1)] kommen immer mehr Daten in die Hände von unberechtigten Dritten. Im Folgenden soll aufgezeigt werden, welche Konsequenzen drohen, wenn persönliche Daten durch eine Ransomware-Attacke gestohlen werden.

I. Arten von Ransomware-Attacken

Um der Frage nachzugehen, welche datenschutzrechtlichen Konsequenzen dem Angegriffenen drohen, muss zunächst nach den unterschiedlichen Formen von Ransomware-Attacken unterschieden werden. Bei der sog. einfachen Ransomware-Attacke werden durch die Angreifer lediglich die Daten verschlüsselt und ein Lösegeld für deren Freigabe gefordert. Zusätzlich wird gedroht, dass die Daten endgültig gelöscht werden, wenn das Lösegeld nicht innerhalb einer bestimmten Frist gezahlt wird. Es kommt in diesem Fall zu keinem Abfluss von – insbesondere persönlichen – Daten. Ein typisches Beispiel hierfür ist die Attacke auf das Lukaskrankenhaus in Neuss im Jahre 2016.[2)] In dieser Konstellation sind datenschutzrechtliche Konsequenzen eher gering, sodass diese im Folgenden nicht näher betrachtet werden sollen und vielmehr die nachfolgend geschilderten Situationen im Fokus stehen.

Die sog. doppelten und dreifachen Erpressungen sind Weiterentwicklungen der einfachen Ransomware-Attacke. Wie bei dieser werden auch bei der doppelten und dreifachen Erpressung die Daten in den IT-Systemen des Angegriffenen verschlüsselt. Im Gegensatz zur einfachen Ransomware-Attacke werden die Daten allerdings auch an den Angreifer gesendet. Dieser droht bei der doppelten Erpressung nicht nur damit, dass bei Nichtzahlung des Lösegelds die Daten des Angegriffenen gelöscht, sondern besonders sensible Daten zusätzlich im Darknet veröffentlicht werden. Insoweit ist es – anders als in der Situation des Lukaskrankenhauses Neuss – nicht mehr alleine ausreichend, die Systeme ohne Zahlung eines Lösegelds über Back-ups wiederherzustellen. In diesem Fall droht dem Angegriffenen noch die Veröffent-

1 Schwartze, USA: Cyberpreise steigen wegen Lösegeldzahlungen, Versicherungsmonitor.de vom 08.02.2021.

2 Siehe zum genauen Ablauf ein Interview mit dem dortigen Geschäftsführer Nicolas Krämer unter https://www.macwelt.de/ratgeber/So-verlief-die-Ransomware-Attacke-im-Lukaskrankenhaus-10682942.html, zuletzt zugegriffen am 22.08.2021.

lichung von sensiblen Daten (z. B. Geschäftsgeheimnisse, persönliche Daten von Kunden usw.), die er meistens unter allen Umständen verhindern möchte.

Bei der dreifachen Erpressung wird hingegen nicht nur ein Lösegeld von dem Angegriffenen gefordert, sondern auch von dessen Kunden. Ein solcher Angriff wurde beispielsweise auf die finnische Klinik für Psychotherapie, Vastaamo, verübt.[3)] Die Angreifer haben von der Klinik Daten von ca. 40.000 Personen gestohlen. Hierunter waren insbesondere Therapietagebücher und andere vertrauliche Daten der Personen. Neben der Klinik erhielten auch die einzelnen Patienten eine E-Mail von den Angreifern mit der Aufforderung, ein Lösegeld zu zahlen, damit deren Daten nicht veröffentlicht werden. Dieses Lösegeld war allerdings signifikant geringer, als dasjenige, was die Angreifer von der Klinik forderten.

II. Datenschutzrechtliche Ansprüche der Betroffenen

Es stellt sich die Frage, welche Ansprüche die Betroffenen gegen den Angegriffenen besitzen, wenn deren persönliche Daten abhandenkommen oder sogar – insbesondere im Internet – veröffentlicht werden. Die Haftung des Angegriffenen richtet sich nach Art. 82 EU-Datenschutz-Grundverordnung (EU-DSGVO) bzw. § 83 Bundesdatenschutzgesetz (BDSG). Hiernach ist er den Betroffenen zur Erstattung des durch die Datenschutzverletzung verursachten materiellen und immateriellen Schadens verpflichtet. Dies gilt nicht, soweit ihn kein Verschulden an der Verletzung trifft.

Die materiellen Schäden werden von den Betroffenen in der Praxis nur schwer nachzuweisen sein. Denkbar ist, dass sie aufgrund der Veröffentlichung ihrer persönlichen Daten einen Job nicht bekommen oder verlieren oder ihnen ein Kredit versagt wird. Allerdings wird in diesen Situationen nur schwer nachzuweisen sein, dass die entsprechende Entscheidung des Arbeitgebers bzw. der Bank kausal auf der Veröffentlichung der gestohlenen Daten beruht. Anders kann es hingegen bei der dreifachen Erpressung aussehen. Zahlt hier der Betroffene das geforderte Lösegeld, könnte dies grundsätzlich ein materieller Schaden sein, den er vom Angegriffenen erstattet verlangen kann.

In der Praxis hat die Möglichkeit, einen immateriellen Schaden zu fordern, ein größeres Gewicht. Ähnlich wie beim Schmerzensgeld bei Personenschäden wird sich hier über kurz oder lang anhand der Rechtsprechung ein Katalog entwickeln, in welcher Höhe Betroffenen ein immaterieller Schaden zusteht, wenn deren persönliche Daten veröffentlicht werden. Aus Sicht des Angegriffenen ist dies insbesondere dann gefährlich, wenn Daten von einer Vielzahl von Personen gestohlen werden. Nehmen wir das Beispiel der finnischen Klinik Vastaamo. Sollten alle Daten der 40.000 Personen veröffentlicht worden sein und jedem Patienten

[4] Das LG Darmstadt, Urt. v. 26.5.2020 – 13 O 244/19 hat beispielsweise bei der Weitergabe von Daten an Dritte einen immateriellen Schaden des Betroffenen in Höhe von 1.000 Euro angenommen.

Foto: Ken Schluchtmann, diephotodesigner.de

ein immaterieller Schaden von lediglich 500 Euro zugesprochen werden,[4] müsste die Klinik alleine für diese Schadenposition 20 Mio. Euro aufwenden.

III. Eigenschäden nach der EU-DSGVO

Die EU-DSGVO gewährt allerdings nicht nur den Betroffenen Schadensersatzansprüche, sondern deren Regelungen können auch zu Eigenschäden beim Angegriffenen führen. So sieht Art. 34 EU-DSGVO bzw. § 66 BDSG vor, dass unter bestimmten Umständen die Betroffenen über eine eingetretene Datenschutzverletzung zu informieren sind. Hierdurch entstehen beim Angegriffenen Kosten für die Benachrichtigung dieser Personen, z. B. für die Feststellung der betroffenen Personen, die Versendung der Benachrichtigung oder damit verbundene Rechtsberatungskosten.

Desweiteren ist in Art. 33 EU-DSGVO bzw. § 65 BDSG geregelt, dass die zuständige Datenschutzbehörde unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu informieren ist. Diese Benachrichtigung hat in der Regel innerhalb von 72 Stunden nach der Kenntnis von der Verletzung zu erfolgen. Insoweit ist bei der doppelten und dreifachen Erpressung in der Regel die zuständige Datenschutzbehörde zu informieren. Hierdurch können weitere Eigenschäden beim Angegriffenen entstehen, insbesondere im Zusammenhang mit einer rechtlichen Beratung und Vertretung gegenüber der Behörde.

IV. Bußgelder

Auch Bußgelder können beim Abhandenkommen von persönlichen Daten eine Rolle spielen, insbesondere dann, wenn diese Daten nicht ordnungsgemäß gesichert wurden. Solche Bußgelder können nach Art. 83 EU-DSGVO verhängt werden. Die Höhe richtet sich danach, welche konkreten Pflichten der EU-DSGVO verletzt worden sind. Im Zusammenhang mit dem unberechtigten Zugriff von Unberechtigten auf persönliche Daten wurden von der zuständigen deutschen Aufsichtsbehörde gegen das Telekommunikationsunternehmen 1&1 beispielsweise ein Bußgeld in Höhe von fast 10 Mio. Euro verhängt, was allerdings vom LG Bonn auf 900.000 Euro reduziert wurde.[5] Desweiteren wurde der Knuddels GmbH & Co. KG in Deutschland ein Bußgeld in Höhe von 20.000 Euro auferlegt, weil das Unternehmen persönliche Daten nicht ausreichend gesichert und damit die Entwendung dieser Daten durch Hacker ermöglicht hatte.[6] Im Ausland werden teilweise höhere Bußgelder bei Entwendung von unzureichend gesicherten Daten durch Hacker verhängt. So belegte beispielsweise die britische Aufsichtsbehörde das Unternehmen Marriott International Inc mit einem Bußgeld von knapp 20 Mio. Euro. Hintergrund war, dass Hacker über einen längeren Zeitraum persönliche Daten von ca. 339 Mio. Gästen entwendeten.[7]

Die Höhe des Bußgelds hängt von den Umständen des Einzelfalls ab, insbesondere der Schwere der Verstöße. Der Fall der Knuddels GmbH & Co. KG zeigt aber, dass eine Kooperation mit den Datenschutzbehörden auch Einfluss auf die Höhe des Bußgelds haben kann. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat die sehr gute Zusammenarbeit des Unternehmens ausdrücklich bußgeldreduzierend berücksichtigt.

Sollte ein Bußgeld nach der EU-DSGVO verhängt werden, stellt sich auch die Frage, inwieweit dies versichert werden kann. In Deutschland ist die Absicherungsmöglichkeit derzeit als unklar zu bezeichnen. Es gibt keine gesetzliche Regelung, die die Übernahme von Bußgeldern durch Versicherer ausdrücklich verbietet, noch sie ausdrücklich erlaubt. In der juristischen Literatur ist daher derzeit umstritten, ob ein Versicherer Bußgelder anstelle des Beschuldigten zahlen kann. Vor diesem Hintergrund ist nicht sicher, ob die Übernahme von Bußgeldern in Deutschland abgesichert werden kann. Allerdings ist die Übernahme von Kosten, um sich gegen das verhängte Bußgeld zu verteidigen, durch einen Versicherer auch in Deutschland unproblematisch. Eine solche Möglichkeit ist in Rechtsschutzversicherungsprodukten schon seit langer Zeit vorgesehen. Lediglich für den Fall, dass der Beschuldigte rechtskräftig bezüglich einer Vorsatztat verurteilt wird, müssen die Abwehrkosten wohl durch den Versicherer zurückgefordert werden.

FAZIT

Durch Ransomware-Attacken drohen den Angegriffenen erhebliche Schäden. Zu nennen sind hier natürlich die dadurch verursachten Betriebsunterbrechungsschäden, die Kosten von IT-Forensikern und die Schäden durch die eventuelle Zahlung von Lösegeldern. Nicht unbeachtet soll allerdings bleiben, dass insbesondere bei der doppelten und dreifachen Erpressung auch datenschutzrechtliche Schäden drohen. Hier sind insbesondere die immateriellen Schäden der Betroffenen, deren persönliche Daten gestohlen und im Internet veröffentlich werden, die Kosten im Zusammenhang mit der Benachrichtigung der Datenschutzbehörde und der Betroffenen und mögliche Bußgelder zu nennen. Insbesondere erstgenannte Schäden können in der Situation, in denen Daten von einer Vielzahl von Personen abhandenkommen, einen hohen Betrag ausmachen. Insoweit ist bei dem Abschluss einer Versicherung auch an diese Schäden zu denken.

Autor

Prof. Dr. Michael Fortmann, LL.M.
Institut für Versicherungswesen Versicherungsrecht und Haftpflichtversicherung
Technische Hochschule Köln, Campus Südstadt
michael.fortmann@th-koeln.de

[3] Siehe hierzu beispielsweise den Bericht unter https://www.dfg-ev.de/news/6226/der-vastaamo-skandal-immer-noch-nicht-geklart, zuletzt zugegriffen am 22.08.2021.
[5] LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20.
[6] Pressemitteilung des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg vom 22.11.2018 (abzurufen unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/, letzter Zugriff am 22.08.2021).
[7] Penalty Notice des ico vom 30.10.2020 (abzurufen unter: https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf, letzter Zugriff am 22.08.2021).
[8] Armbrüster/Schilbach, r+s 2016, 109 (110 ff.)