Editorial – Grußwort des Forschungsprojektleiters von »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur dritten Ausgabe des BayWiDI-Magazins.

Thema: Cyberkriminalität

In der dritten Ausgabe des BayWiDI-Magazins werden Ihnen wieder interessante und aktuelle Themen aus dem Bereich der IT-Sicherheit vorgestellt.

Im ersten Beitrag dieses Magazins mit dem Titel „Unternehmensbezogene Cyberkriminalität – Eine nicht zu unterschätzende Gefahr“ wird eine Kehrseite der Digitalisierung beleuchtet: die steigende Zahl der Cyberangriffe auf Unternehmen. Der Beitrag definiert den Begriff der Cyberkriminalität und nimmt eine Einordnung verschiedener Arten von Cyberattacken vor. Es werden wirtschaftliche Schäden in den Blickpunkt gestellt und verschiedene Risikofaktoren aufgezeigt. Ebenso wird ein Ausblick auf die mögliche Strafbarkeit derartiger Angriffe geworfen.

Der zweite Beitrag mit dem Titel »Unternehmensbezogene Cyberkriminalität – Eine juristische Betrachtung« schließt sich thematisch nahtlos an den vorangegangenen Beitrag an. Der Artikel soll Unternehmen eine erste Handreichung bieten, welche Verhaltenspflichten vor oder nach einem eingetretenen IT-Sicherheitsvorfall rechtlich bzw. im eigenen Interesse einzuhalten sind. Im Nachgang wird dem Leser ein kurzer Einblick in mögliche Haftungsgrundlagen geben, wobei sowohl auf die Sicht des Unternehmens als auch Dritter abgestellt wird.

Nun wünsche ich Ihnen eine interessante Lektüre der dritten Ausgabe des BayWiDI-Magazins!

Ihr Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

Inhalt

In eigener Sache

Ich habe die große Ehre und Freude, zum 1.10.2019 an die TU München auf den dort für mich eingerichteten Lehrstuhl für Recht und Sicherheit der Digitalisierung zu wechseln (hierzu die PM: https://www.tum.de/nc/die-tum/aktuelles/pressemitteilungen/details/35569/). Dort werde ich als Mitglied der TUM School of Governance und der Fakultät für Informatik meine interdisziplinäre Forschung fortsetzen. Der Universität Passau bleibe ich als Affiliate Professor und Leiter der Forschungsstelle für IT-Recht und Netzpolitik erhalten, deren Forschungsprojekte (wie BayWiDI) weitergeführt werden. Sie erreichen uns deshalb wie gewohnt!

Prof. Dr. Dirk Heckmann

Unternehmensbezogene Cyberkriminalität – Eine nicht zu unterschätzende Gefahr

Die voranschreitende Digitalisierung bietet viele Chancen und Möglichkeiten, sowohl für Unternehmen, als auch für Privatpersonen. Jedoch werden durch diese technischen und wirtschaftlichen Neuerungen auch unliebsame Nebeneffekte und Gefahren geschaffen. Die Zahl der Cyberangriffe auf informationstechnische Systeme nimmt stetig zu.[1]

Eine kaum greifbare Anzahl an Firmen wurde bereits Ziel von Cyberattacken, zu nennen sind nur beispielhaft Sony, Deutsche Bahn, Deutsche Telekom, Uber oder LinkedIn.[2] Ein medial besonders hervorgehobener Cyberangriff lief über die Erpressersoftware „WannaCry", welche im Mai 2017 hunderttaussende Systeme zum Erliegen brachte.[3] Großes Aufsehen erregte auch die Phishing-Attacke auf die Abteilung der Lohnbuchhaltung von Snapchat im Jahr 2016. Durch ein falsches CEO-Profil wurden Mitarbeiter dazu aufgefordert geheime Daten über Lohnabrechnungen herauszugeben.[4]

In jüngster Vergangenheit hat auch die Schadsoftware „Emotet" immer wieder zu großen Schäden geführt. Diese Schadsoftware liest Kontaktdaten der betroffenen Benutzer aus und versendet so an deren Kontakte teilweise täuschend echt wirkende E-Mails. Oft wird dann nichtsahnend ein Anhang geöffnet und die Schadsoftware infiziert den nächsten Rechner und kann sich weiter ausbreiten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt eingehend vor den Gefahren von „Emotet".[5]

Definition

Nach der Definition des Bundeskriminalamts (BKA) umfasst der Begriff der Cyberkriminalität Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten oder die mittels dieser Informationstechnik begangen werden.[6]

Cyberkriminalität mit wirtschaftlichem Bezug

Cyberkriminelle haben es oft auf kleine und mittelständische Unternehmen abgesehen, da sich diese – im Vergleich zu den großen Unternehmen – zumeist schlecht oder gar nicht gegen derartige Angriffe schützen. Besonders betroffen sind die Automobil-, Luftfahrzeug-, Schiff- und Maschinenbaubranchen.[7] In Deutschland waren in den Jahren 2015 und 2016 mehr als die Hälfte der Unternehmen Opfer von Cyberattacken.[8]

Die Mehrheit dieser Angriffe ist im Kern auf Ausspähung von Konkurrenten und Industriespionage zurückzuführen. Somit stellen vor allem ausländische Konkurrenten einen eklatanten Risikofaktor dar. Diese wollen sich in erster Linie illegal Kundendaten, Marktinformationen und Unternehmensstrategien verschaffen.[9] Jedoch sind auch staatliche Geheimdienste involviert und versuchen für sich bzw. die im Hintergrund agierenden Staaten durch Cyberattacken auf andere Staaten oder Unternehmen Informationen abzugreifen. Doch stehen nicht nur Staatsgeheimnisse im Fokus. Ferner geht es schlichtweg um die Generierung wirtschaftlicher Wettbewerbsvorteile.[10]

Einordnung von Cyberattacken

Um eine Cyberattacke korrekt einordnen zu können, ist deren Zielrichtung zu betrachten. Urheber dieser Angriffe können Einzeltäter oder Banden, Konkurrenzunternehmen oder gar ausländische Geheimdienste sein.[11]

Ist der Angriff ausschließlich darauf gerichtet, in den entsprechenden Systemen Schäden anzurichten, so wird dies in der Regel durch Würmer, Viren, DoS- (Denial of Service) oder DDoS-Attacken (Distributed Denial of Service) versucht werden. Dies soll in erster Linie den Betrieb und die Infrastruktur des angegriffenen Unternehmens beeinträchtigen oder komplett lahmlegen.[12]

1 *BMI*, https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html zuletzt abgerufen am 23.08.2019.

2 *finanzchef24*, https://www.finanzchef24.de/sites/default/files/media/versicherung/cybercrime-risikogruppe-deutscher-mittelstand-finanzchef24.pdf, Seite 2, zuletzt abgerufen am 26.08.2019.

3 *Beukelmann*: Cyber-Attacken – Erscheinungsformen, Strafbarkeit und Prävention, NJW-Spezial 2017, 376.

4 *Werne*, der Bank Blog, https://www.der-bank-blog.de/mensch-cybercrime/trends/38675/ zuletzt abgerufen am 26.08.2019.

5 *BSI*, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html zuletzt abgerufen am 23.08.2019.

6 *BKA* , https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html zuletzt abgerufen am 26.08.2019.

7 *Wilke*, Der strafrechtliche Schutz von Daten vor Konkurrenzausspähung und Wirtschaftsspionage, NZWiSt 2019, 168, zuletzt abgerufen am 26.08.2019.

8 *Bitkom*, https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf, Seite 2, zuletzt abgerufen am 26.08.2019.

9 *Wilke*, Der strafrechtliche Schutz von Daten vor Konkurrenzausspähung und Wirtschaftsspionage, NZWiSt 2019, 168.

10 *Wilke*, Der strafrechtliche Schutz von Daten vor Konkurrenzausspähung und Wirtschaftsspionage, NZWiSt 2019, 168, 172.

11 *Mehrbrey/Schreibauer*, Haftungsverhältnisse bei Cyberangriffen - Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75; vgl. auch Wilke, Der strafrechtliche Schutz von Daten vor Konkurrenzausspähung und Wirtschaftsspionage, NZWiSt 2019, 168, 173.

12 *Mehrbrey/Schreibauer*, Haftungsverhältnisse bei Cyberangriffen - Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75.

Bei einer Erpressung mittels eines Cyberangriffs fordern Hacker eine Geldzahlung, ein Handeln oder ein Unterlassen von den betroffenen Personen oder Unternehmen, um den Angriff abzubrechen. Dabei nutzen Hacker auch DoS-, DDoS-Attacken und Ransomware.[13] Unter Ransomware fällt auch der bereits angesprochene Krypto-Trojaner „WannaCry“. Damals wurden IT-Systeme von Unternehmen durch eine Sicherheitslücke im Windows Betriebssystem kompromittiert, deren Daten verschlüsselt und Lösegeld erpresst.[14]

Zum Zwecke der unternehmensbezogenen Spionage greifen Hacker vorsätzlich auf Datenspeicher des Unternehmens zu, um so Betriebs- und Geschäftsdaten zu erhalten. Dadurch entstehen auf illegale Weise Wettbewerbsvorteile gegenüber den betroffenen Unternehmen.[15]

Hacker, die mit dem Ziel agieren, sich Zugangsdaten zu eigenen Zwecken zu verschaffen, setzen oft Methoden wie das sogenannte Phishing oder Pharming ein. Dadurch können Benutzernamen, Passwörter und zum Beispiel auch Kreditkarteninformationen beschafft werden.[16]

Technischer Ablauf einer Cyberattacke

Ein besonders häufiges Angriffsszenario ist der Versand einer infizierten E-Mail. Wird diese oder deren Anhang geöffnet, wird im Hintergrund der Download der eigentlichen Schadsoftware eingeleitet. Oft hat der Angreifer nur durch einmaliges Öffnen anschließend Zugriff auf das gesamte Netzwerk der Firma.[17]

E-Mails kommen auch beim Phishing zum Einsatz. Es werden etwa Webseiten und E-Mails von bekannten Unternehmen gefälscht, um den Benutzer dazu zu bringen, seine Daten preiszugeben.[18]

Verbreitete Methode ist außerdem der Einsatz von Botnetzen, wobei Täter, vom Nutzer unbemerkt, Schadsoftware auf dessen Computer installieren. Diese Schadsoftware soll dann viele weitere PCs infizieren, welche der Angreifer aus der Ferne steuern kann.[19]

Entstehende Schäden durch Cyberattacken

Durch Datendiebstahl und Produktionsunterbrechungen werden erhebliche Schäden, vor allem finanzieller Art, verursacht. Die meisten kleineren und mittelgroßen Unternehmen schätzen ihr eigenes Risiko, Opfer einer Cyberattacke zu werden, viel zu gering ein.[20] Oftmals sind aber gerade diese Unternehmen im Fokus von Hackern, da unternehmensseitig kaum in die IT-Sicherheit investiert wird.[21]

Zu den am meisten auftretenden Schäden zählen zunächst die Aufklärungskosten und Kosten zur Datenwiederherstellung. Darunter fällt auch, dass viele Unternehmen, infolge eines Angriffs, ihre Soft- und Hardware ersetzen müssen.[22]

Des Weiteren ist mit Betriebsunterbrechungen und damit einhergehenden Umsatzeinbußen zu rechnen (z.B. durch Produktionsstillstand oder Ausfall des IT-Systems).[23]

Zu beachten sind auch mögliche Reputationsschäden eines Unternehmens, das nach einer Cyberattacke zunächst einmal seinen Ruf wiederherstellen muss. Möglich ist auch ein erheblicher Diebstahl von Kundendaten oder vertraulichen Unternehmensdaten.[24]

Sogar die körperliche Sicherheit von Menschen kann gefährdet werden. Es gab bereits Fälle von Hackerangriffen auf Krankenhäuser, überdies ist es sogar möglich, funkgesteuerte Maschinen in einem Unternehmen zu hacken und willkürlich fernzusteuern.[25]

13 *Mehrbrey/Schreibauer*, Haftungsverhältnisse bei Cyberangriffen - Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75.

14 *Beukelmann*, Cyber-Attacken – Erscheinungsformen, Strafbarkeit und Prävention, NJW-Spezial 2017, 376.

15 *Mehrbrey/Schreibauer*, Haftungsverhältnisse bei Cyberangriffen - Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75.

16 *Mehrbrey/Schreibauer*, Haftungsverhältnisse bei Cyberangriffen - Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75, 76.

17 *GDV*, https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbf-b7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf Seiten 4 u. 5 zuletzt abgerufen am 28.08.2019.

18 *Mehrbrey/Schreibauer*, Haftungsverhältnisse bei Cyberangriffen - Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75, 76.

19 *Beukelmann*, Cyber-Attacken – Erscheinungsformen, Strafbarkeit und Prävention, NJW-Spezial 2017, 376.

20 *GDV*, https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbf-b7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf, Seite 8 zuletzt abgerufen am 28.08.2019.

21 *GDV*, https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbf-b7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf, Seite 9 zuletzt abgerufen am 28.08.2019.

22 *GDV*, https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbf-b7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf, Seite 11 zuletzt abgerufen am 28.08.2019.

23 *GDV*, https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbf-b7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf, Seiten 4 und 11 zuletzt abgerufen am 28.08.2019.

24 *Noerr LLP*, https://www.noerr.com/de/newsroom/news/Cyberangriff%20und%20Datendiebstahl zuletzt abgerufen am 29.08.2019.

25 *Tremmel*, https://www.golem.de/news/medizin-schadsoftware-legt-ueber-zehn-krankenhaeuser-lahm-1907-142639.html zuletzt abgerufen am 28.08.2019.

Risikofaktoren

Die Gründe für die Zunahme der Cyberattacken auf Unternehmen liegt vor allem in der stetig voranschreitenden Digitalisierung. Nicht nur technische Defizite oder mangelnde Softwareupdates sind für erfolgreiche Cyberattacken ausschlaggebend. Hinzu kommen ferner sicherheitsverletzende Handlungen der Mitarbeiter selbst.[26] Diese sollten stets auf aktuelle Sicherheitsgefahren hingewiesen werden sowie sollten ihnen entsprechende Verhaltenskodizes an die Hand gegeben werden, um sämtliche Sicherheitsrisiken zu minimieren. Beispielhaft sei hier nur das Verbot der Vernetzung privater Geräte mit dem Arbeitsnetzwerk oder etwa das Verbot des Öffnens von E-Mail Anhängen bei unbekanntem Absender genannt. Häufig werden untergeordnete Mitarbeiter das Ziel von Cyberattacken via E-Mail, indem diesen suggeriert wird, die E-Mail stamme von einer übergeordneten Person innerhalb des Unternehmens.[27]

Die wohl größte Problematik stellt das sogenannte „Bring Your Own Device (BYOD)"-Konzept dar. Bei BYOD wird in der Regel eine IT-Richtlinie durch das Unternehmen aufgestellt, in der die Anwendungsmöglichkeiten und Vernetzungszulässigkeiten bzgl. der privat seitens der Angestellten angeschafften IT-Geräte verbindlich festgelegt werden. Dies bewirkt einerseits zahlreiche Vorteile in der unternehmerischen Arbeitsumgebung. Die Benutzer sind in der Handhabung ihrer eigenen Geräte in der Regel bereits versiert; dies kann dem Produktionsfluss zum Vorteil gereichen.[28] Andererseits bedeutet es allerdings, dass die Mitarbeiter mit ihren persönlichen Endgeräten Zugriff auf die IT-Infrastruktur des Unternehmens erhalten und folglich Sicherheitsrisiken entstehen.[29] Ebenso drohen Unternehmensdaten unberechtigterweise in die Hände Dritter zu gelangen oder verloren zu gehen, sollte das private Endgerät abhandenkommen.[30]

Strafbarkeit der Angreifer

Je nach Ausführung des Cyberangriffs machen sich die Initiatoren beispielsweise - aber keinesfalls abschließend - strafbar des Ausspähens von Daten (§ 202 a StGB), des Abfangens von Daten (§ 202 b StGB), des Vorbereitens des Ausspähens von Daten (§ 202 c StGB), der Datenhehlerei (§ 202 d StGB), der Datenveränderung (§ 303 a StGB), der Computersabotage (§ 303 b Abs. 1, 2 Alt. 2 StGB) oder auch des Betrugs (§ 263 StGB). In besonders gelagerten Fällen kommt sogar eine Strafbarkeit wegen geheimdienstlicher Agententätigkeit (§ 99 StGB) oder Industriespionage (§ 17 Abs. 2 Nr. 1 AWG und § 42 BDSG) in Betracht.[31]

Fazit

Die Problematik von Cyberattacken im privaten und unternehmerischen Umfeld ist so aktuell wie eh und je. Sowohl Privatanwender als auch Unternehmen sind gehalten sich bezüglich dieser Gefahr zu informieren und geeignete Gegenmaßnahmen zu ergreifen. Von wenig aufwendigen Vorkehrungen wie die stetige Installation aktueller Sicherheitsupdates bis hin zu einer komplexen Umstrukturierung des Unternehmensnetzwerks sind viele Methoden denkbar. Je nach Anwendungsgebiet und Risikobereich sollte man sich im entsprechenden Intensivierungsgrad gegen Cyberattacken absichern. Erfahrungsgemäß sind die Kosten und der Aufwand einer vorherigen Absicherung stets geringer als eine achträgliche Schadensbeseitigung, falls diese überhaupt möglich ist. Von dem zivilrechtlichen Haftungsrisiko ganz zu schweigen. Daher sind Unternehmen gut beraten durch eine angemessene IT-Sicherheit dieses Haftungsrisiko bereits im Vorfeld maximal zu minimieren.

Ass. jur. Thomas Schneck

26 *BKA*, https://www.bka.de/DE/Ihre-Sicherheit/RichtigesVerhalten/Straftate-nImInternet/Wirtschaftsunternehmen/wirtschaftsunternehmen_node.html zuletzt abgerufen am 28.08.2019.

27 *Heckmann* in: Heckmann, jurisPK-Internetrecht, 6. Auflage 2019, Kap. 8, Rn. 194.

28 *Begler*, it-Business, https://www.it-business.de/was-ist-bring-your-own-device-byod-a-651323/ zuletzt abgerufen am 28.08.2019.

29 *Schäfers*, it-Service.Network, https://it-service.network/blog/2018/07/31/bring-your-own-device/ zuletzt abgerufen am 28.08.2019.

30 *Erlach*, zdnet, https://www.zdnet.de/88198260/bring-device-war-gestern-die-zukunft-heisst-lyod/ zuletzt abgerufen am 28.08.2019.

31 *Wilke*, Der strafrechtliche Schutz von Daten durch Konkurrenzausspähung und Wirtschaftsspionage, NZWiSt 2019, 168, 169 ff.

Unternehmensbezogene Cyberkriminalität – Eine juristische Betrachtung

Ziel dieses Beitrags ist es, aufbauend auf der mittels des vorherigen Artikels gewährten, die Grundlagen beleuchtenden Einführung in die Problematik der unternehmensbezogenen Cyberkriminalität, einen ergänzenden Überblick hinsichtlich der Auswirkungen eines möglichen Angriffs zu geben, sowie zusammenhängend damit rechtliche Handlungspflichten und mögliche Haftungsrisiken zu erörtern. Im Anschluss an eine auf die Grundzüge beschränkte Darstellung möglicher unternehmensseitig bestehender Melde- und Informationspflichten folgt eine prägnante Schilderung der wichtigsten Haftungsgrundlagen und Ansprüche.

Der vorliegende Beitrag soll betroffenen Unternehmen als „erste" Handreichung hinsichtlich der Frage dienen, wie im Falle eines Sicherheitsvorfalls idealerweise zu verfahren ist.

Mögliche Folgen und Auswirkungen eines Angriffs

Neben der zeitweisen Verringerung der eigenen Produktivität sowie möglichen Umsatzeinbußen durch Ausfall eines wesentlichen Teils der IT-Infrastruktur, drohen Unternehmen weitere finanzielle Nachteile bedingt durch Reputationsschäden, etwaige Schadensersatzansprüche Betroffener sowie (möglicherweise existenzgefährdende) staatliche Bußgelder. Handelt es sich bei der betroffenen Entität um eine GmbH oder AG drohen überdies Haftungsrisiken für die Geschäftsleitung.

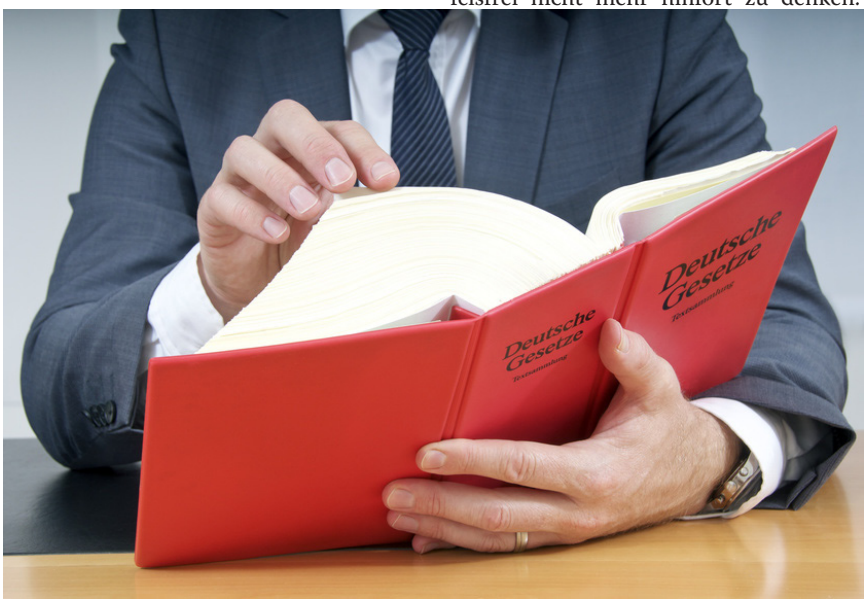
Vorgehensweise

Grundsätzlich gilt es drei wesentliche Kernbereiche in Bezug auf die Gewährleistung und Wiederherstellung von IT-Sicherheitsstrukturen zu betrachten:

- Prävention
- Erkennung
- Reaktion

Vorgehen vor einem Zwischenfall

Wie auch in der analogen Welt gilt, dass es einen hundertprozentigen Schutz gegen sämtliche mögliche Angriffe denklogisch nicht geben kann. Zu vielfältig sind die digitalen Einfallstore und zu unüberschaubar der Kreis denkbarer Angreifer. Dennoch kann der Zugang schädigender Kräfte durch Vorhaltung



geeigneter Maßnahmen eingeschränkt werden. Wenngleich nicht jedem Unternehmen die finanziellen sowie personellen Möglichkeiten zur Verfügung stehen, um die von führenden IT-Unternehmen entwickelten, branchenüblichen Standards einzuhalten, wird – so etwa seitens des Bundeskriminalamts (BKA)[1] – auch finanzschwachen Betrieben empfohlen, jedenfalls folgende Sicherheitsmaßnahmen einzuhalten:

- Installation der bereitgestellten Softwareupdates
- Verwendung einer Firewall
- Verwendung sicherer Passwörter
- Einsatz von Verschlüsselungsmechanismen
- Erstellung regelmäßiger Updates

1 *BKA*, Cybercrime – Handlungsempfehlungen für die Wirtschaft, 2018, S. 13.

Die vorgenannten Sicherungsmittel basieren nicht nur auf rein privatwirtschaftlichen Überlegungen, vielmehr dienen sie gleichfalls der Umsetzung bestehender gesetzlicher Sicherungsmaßnahmen.

Nicht nur in der neueren juristischen Literatur ist – spätestens seit Eröffnung der insbesondere medial sowie seitens der Fachliteratur ausgetragenen Debatte um die EU-Datenschutzgrundverordnung (DS-GVO) – ein Themenbereich zweifelsfrei nicht mehr hinfort zu denken: Das Datenschutzrecht. Auch und natürlich besonders im Rahmen der präventiven IT-Sicherheit müssen nunmehr die Vorgaben der DS-GVO Beachtung finden. Dies gilt namentlich deshalb, weil unternehmensbezogene IT-Systeme zumeist (jedenfalls auch) personenbezogene Daten verarbeiten. Relevanteste Norm in diesem Zusammenhang ist Art. 32 DS-GVO. Dieser legt dem für die Datenverarbeitung Verantwortlichen (etwa das Unternehmen) in Art. 32 Abs. 1 DS-GVO die Verpflichtung auf, geeignete technische und organisatorische Maßnahmen (sog. TOMs) zu ergreifen, um für die verarbeiteten personenbezogenen Daten ein angemessenes Schutzniveau

zu gewährleisten. Die DS-GVO steht insoweit unter der (unausgesprochenen jedoch selbsterklärenden) Prämisse, dass es effektiven Datenschutz niemals ohne Datensicherheit, mithin ebenfalls niemals ohne IT-Sicherheit, geben kann.[2]

Bei der Festlegung der notwendigen TOMs hat das Unternehmen unter anderem sämtliche Risiken zu berücksichtigen, die für die im Einzelfall betroffenen Daten zu befürchten sind. Einen ersten Anhaltspunkt für den Einsatz in der Praxis bieten die (nicht abschließenden) Beispielsmaßnahmen in Art. 32 Abs. 1 lit. a) bis d) DS-GVO. Hier zeigen sich bereits erste Übereinstimmungen mit den oben aufgeführten IT-Sicherheitsmaßnahmen: beispielsweise das Instrument der Verschlüsselung. Ferner erlangt der Grundsatz der Verhältnismäßigkeit Geltung. Demgemäß sind nicht alle theoretisch denkbaren IT-sicherheitsbezogenen Maßnahmen unternehmensseitig zu ergreifen, sondern nur all solche, die entsprechend einer Abwägung, als angemessen zu bewerten sind.[3] Abzuwägen sind insofern z.B. die Schwere drohender Risiken, deren Eintrittswahrscheinlichkeit sowie veranschlagte Implementierungskosten.[4]

Im weitesten Sinne ebenfalls als präventive IT-Sicherheitsmaßnahme kann die in Art. 35 DS-GVO geregelte Datenschutz-Folgeabschätzung klassifiziert werden. Im Falle eines hohen Schadenspotentials für die verarbeiteten personenbezogenen Daten dient diese dazu, Risiken für die Rechte der Betroffenen frühzeitig zu erkennen sowie im Einzelfall geeignete Maßnahmen zur Datensicherung zu ergreifen.[5] Sofern nach Art. 37 DS-GVO ein Datenschutzbeauftragter zu benennen ist, hat auch dieser im erweiterten Sinne originäre IT-Sicherheitsaufgaben wahrzunehmen.

Neben der DS-GVO trifft auf europäischer Ebene die NIS-Richtlinie (RL EU/2016/1148) Maßnahmen zur Gewährleistung eines hohen IT-Sicherheitsniveaus. Während die DS-GVO bereits auf Grund ihres Verordnungs-Charakters unmittelbare Geltung erlangte, bedurfte es zur Wirksamkeit der NIS-Richtlinie eines gesonderten nationalen Umsetzungsaktes. Ein wesentlicher Teil der Richtlinie wurde dabei im Rahmen des BSIG umgesetzt. Im Unterschied zum europäischen Datenschutzrecht (d.h. der DS-GVO) unterfallen jedoch nicht alle Unternehmen den strengen Regelungen des BSIG. Den wesentlichen Adressatenkreis bilden vielmehr nur Betreiber Kritischer Infrastrukturen (KRITIS). Eine genaue Begriffsbestimmung enthält § 10 Abs. 2 BSIG bzw. ergänzend die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV).

Unabhängig von den verarbeiteten Daten müssen KRITIS-Betreiber nach § 8a Abs. 1 BSIG auch ohne konkreten Sicherheitsvorfall bereits im Vorfeld dem Stand der Technik entsprechende angemessene TOMs zum Schutz der IT-Sicherheit vorhalten. Erklärte Zielsetzung muss insoweit sein, die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der eigenen IT-Infrastruktur dauerhaft zu gewährleisten. Wenngleich die Einhaltung dieser Vorgaben naturgemäß bereits im Eigeninteresse des Unternehmens liegt, um einen reibungslosen Betriebsablauf zu garantieren bzw. einer zivilrechtlichen Haftung gegenüber Vertragspartnern zu entgehen, sind sämtliche der im BSIG enthaltenen IT-Sicherheitsanforderungen allesamt überdies bußgeldbewehrt.

Neben Regelungen für KRITIS-Anbieter enthält das BSIG in § 8c BSIG gesonderte Regelungen für Anbieter digitaler Dienste. Unter diese Kategorie fallen gemäß § 2 Abs. 11 und 12 BSIG Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Cloud-Computing-Diensten. Diese Anbieter haben nach § 8c Abs. 1 BSIG ebenfalls geeignete, verhältnismäßige und mit denen der KRITIS-Betreiber vergleichbare TOMs zu treffen.[6] Anzumerken ist, dass Kleinst- und Kleinunternehmen nach § 8d Abs. 4 BSIG diesen gesetzlichen Anforderungen nicht unterstehen. Hierbei handelt es sich um solche Unternehmen, die weniger als 50 Personen beschäftigen und einen Jahresumsatz von weniger als 10 Millionen Euro generieren.[7] Im Hinblick auf mögliche Cybersecurity-Angriffe ist es jedoch trotz fehlender gesetzlicher Verpflichtung auch kleineren Unternehmen zu raten, die durch das BSIG normierten Vorgaben zumindest als Orientierung zu begreifen und somit die ihnen (finanziell) verfügbaren Systeme vorzuhalten.

Rechtlich problematisch gestaltet sich insofern die auf den ersten Blick durchaus vorteilhaft erscheinende Möglichkeit der Einrichtung eines Angriffserkennungssystems. Insbesondere die Frage nach der Zulässigkeit eines solchen Systems unter Beachtung des Telekommunikationsgesetzes (TKG), hier vor allem § 88 TKG, bedarf besonderer Aufmerksamkeit. Dem Wortlaut des § 88 Abs. 1 TKG nach unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Beachtlich ist, dass hiervon auch erfolglose Verbindungsversuche erfasst sind. § 88 Abs. 2 TKG macht allerdings deutlich, dass nur die Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet sind. Diensteanbieter in diesem Sinne sind TK-Diensteanbieter gem. § 3 Nr. 6 TKG. Fraglich ist nun, ob der Einsatz von Angriffserkennungssystemen mit dem von § 88 TKG statuierten Inhalt vereinbar ist, denn die Verwendung von Angriffserkennungssystemen könnte einen Eingriff in das Fernmeldegeheimnis darstellen.

Möglicherweise könnte der Einsatz solcher Systeme auf § 100 Abs. 1 Satz 1 TKG gestützt werden. Demnach darf ein Diensteanbieter, soweit erforderlich, die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation

2 *Mantz* in Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 32 Rn. 5.

3 *Mantz* in Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 32 Rn. 10.

4 *Mantz* in Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 32 Rn. 10.

5 *Schwendemann* in Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 35 Rn. 1.

6 *Voigt*, IT-Sicherheitsrecht, 1. Aufl. 2018, Rn. 393.

7 *Voigt*, IT-Sicherheitsrecht, 1. Aufl. 2018, Rn. 388.

zwischen Empfänger und Sender notwendig sind, erheben und verwenden, um Störungen oder Fehler am Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Die Verarbeitung von Inhaltsdaten scheint vom Gesetzgeber jedoch gerade nicht gewollt zu sein.[8] Somit kann § 100 Abs. 1 Satz TKG 1 i.V.m. § 109 TKG nicht als Rechtsgrundlage herangezogen werden.

Möglicherweise als Rechtsgrundlage in Betracht kommt ferner § 88 Abs. 3 Satz 1 TKG.[9] Dieser normiert ein Verbot dahingehend, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Im Ergebnis können sich TK-Diensteanbieter also Informationen über den Inhalt der Telekommunikation verschaffen, sofern dies für den Schutz ihrer technischen Systeme erforderlich ist.[10] Umstritten ist jedoch, wann eine solche Erforderlichkeit zu bejahen ist. Schwierigkeiten in der Praxis sind die Folge dieses Problems. So ist etwa bislang nicht abschließend geklärt, ob Viren- und Spamfilter unter den Begriff der Erforderlichkeit fallen.[11]

Neben der Vereinbarkeit mit dem TKG ist der Einsatzes von Angriffserkennungssystemen nach der DS-GVO zweifelsbehaftet. Denn die Verarbeitung personenbezogener Daten müsste auch aus datenschutzrechtlicher Perspektive zulässig sein. Dies ist grundsätzlich jedenfalls immer dann der Fall, wenn eine Norm die Verarbeitung ausdrücklich zulässt.[12] Als Rechtsgrundlage in Betracht kommt insoweit Art. 6 Abs. 1 lit. c) DS-GVO. Dagegen kommen die Bestimmungen der NIS-RL in Ermangelung unmittelbarer Wirkung nicht in Betracht; und auch das BSIG ermächtigt mit (dem von der Rechtsfolge her zwar grundsätzlich passenden) § 5 BSIG (Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes) nur das BSI zum Tätigwerden und dies auch nur hinsichtlich der Bundesverwaltung.[13] Allerdings könnten § 8a BSIG und § 8c BSIG als rechtliche Verpflichtung und damit Rechtsgrundlage des für die Verarbeitung Verantwortlichen im Sinne des Art. 6 Abs. 1 lit. c) DS-GVO fungieren.[14] Jedenfalls aber müsste unternehmensseitig ein berechtigtes Interesse für den Einsatz des Angriffserkennungssystems gegeben sein. Die Informations- und Netzsicherheit stellen grundsätzlich ein berechtigtes Interesse in diesem Sinne dar.[15]

Auf personeller Ebene bedacht werden sollte der Aspekt der Verhinderung eines Cyberangriffs mithilfe eigener Mitarbeiter. Letztere sollten grundsätzlich (wiederholt) mit sämtlichen Sicherheitsvorkehrungen vertraut gemacht werden. Ihr Sicherheitsverständnis muss unter anderem dahingehend gefördert werden, entsprechende Angriffe möglichst frühzeitig zu erkennen, um notwendige Gegenmaßnahmen (selbständig) routiniert und zeitnah einleiten zu können. Des Weiteren sollte innerhalb des Unternehmens ein IT-Sicherheitsbeauftragter benannt und bekannt gemacht werden. Ferner ist es ratsam, einen Notfallplan zu erstellen, der konkret und verständlich erläutert, welche Maßnahmen wie einzuleiten sind, sowie welcher Mitarbeiter für welche Aufgaben zuständig ist. Auch dieser Plan ist bekannt zu machen, regelmäßige Aktualisierungen und Anpassungen basierend auf technischen / rechtlichen Neuerungen sollten zudem selbstverständlich sein. Insbesondere auch die Erfahrungswerte identifizierter und analysierter Cyberangriffe können und sollten genutzt werden, um zukünftigen Gefahrensituationen gestärkt zu begegnen bzw. Sicherheitslücken zu schließen und somit Infektionen im Vorfeld zu verhindern. Wichtige Daten bzw. Akten sind separat und gut verschlossen aufzubewahren, sodass sie nicht zur freien Verfügbarkeit über das (Unternehmens-) Netz stehen.

Weitere Handlungsempfehlungen sind auf der Seite des Bundeskriminalsamts zu finden.[16]

Vorgehen vor einem Zwischenfall

Kommt es in Folge eines Cyber-Angriffs zu einer Verletzung der Datensicherheit und auf Grund dessen zu einem Abfluss bzw. einer Verletzung personenbezogener Daten, unterliegt das betroffene Unternehmen Meldepflichten nach der DS-GVO. Konkret handelt es sich dabei um die Pflicht zur Information der Aufsichtsbehörde, Art. 33 DS-GVO, sowie des Betroffenen Art. 34 DS-GVO. Grundsätzlich ist die Verletzung nach Art. 33 Abs. 1 Satz 1 DS-GVO unverzüglich, d.h. ohne schuldhaftes Zögern[17], jedoch möglichst innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden. Diese, gerade bei schwer aufzuarbeitenden Sicherheitsvorfällen, kurze Meldefrist soll negative Auswirkungen

8 *Krügel*, MMR 2017, 795, 797.

9 *Krügel*, MMR 2017, 795, 797.

10 *Krügel*, MMR 2017, 795, 797.

11 *Krügel*, MMR 2017, 795, 797.

12 *Krügel*, MMR 2017, 795, 798.

13 *Krügel*, MMR 2017, 795, 798.

14 *Krügel*, MMR 2017, 795, 798.

15 Vertiefend zum Einsatz von Angriffserkennungssystemen *Krügel*, MMR 2017, 795, 798

16 BKA, Cybercrime - Handlungsempfehlungen für die Wirtschaft, abrufbar unter: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Wirtschaftsunternehmen/wirtschaftsunternehmen_node.html, zuletzt abgerufen am 09.09.2019.

17 *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 33 Rn. 16.

für die Rechte der Betroffenen vermeiden bzw. diese schnellstmöglich beenden.[18] Die Vorgabe von 72 Stunden bildet das Maximum, dessen Ausschöpfung im Einzelfall von der Schwere des Angriffs und der Verletzungstiefe der personenbezogenen Daten abhängt.[19] Als Faustregel gilt insoweit: Je größer der Eingriff ist, desto kürzer ist die Frist.[20] Unternehmen ist dringend davon abzuraten, insbesondere im Hinblick auf drohende Bußgelder, diese Frist zu überschreiten. Um dies sicherzustellen kann es hilfreich sein, in die Unternehmensstruktur spezifische Data Breach Notification Policies oder ein hierauf abgestimmtes Standard Operating Procedure einzuführen.[21]

Die genannte Mitteilungspflicht an die Behörde entfällt gem. Art. 33 Abs. 1 Satz 1 DS-GVO, wenn kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Letzteres beurteilt sich entsprechend einer unternehmensseitig eigenverantwortlich erfolgenden Prognoseentscheidung, wobei die Aufsichtsbehörde diese Einschätzung nicht teilen muss.[22] Folglich verbleibt die Gefahr einer Fehleinschätzung und damit einhergehender Unannehmlichkeiten für das Unternehmen.

Gelangt ein Unternehmen nach einem Sicherheitsvorfall sogar zu der Einschätzung, dass ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen eingetreten ist, hat es nicht nur die Pflicht, die Aufsichtsbehörde zu informieren, es bedarf überdies auch einer unverzüglichen Information der Betroffenen, Art. 34 Abs. 1 DS-GVO. Diese Pflicht entfällt gem. Art. 34 Abs. 3 DS-GVO unter anderem dann, wenn das Unternehmen geeignete TOMs zur Eindämmung drohender Risiken getroffen hat oder eine der weiteren in Art. 34 Abs. 3 lit. a) bis c) normierten Voraussetzungen vorliegt.[23] Diese Einschränkung verdeutlicht abermals, dass präventive Maßnahmen im originären Interesse von Unternehmen liegen. Kann ein Unternehmen durch den Nachweis geeigneter Maßnahmen eine Benachrichtigungspflicht abwenden, hat es keine negativen Auswirkungen seitens seiner Kunden oder von Dritten zu befürchten.

Abweichend von der Meldepflicht der DS-GVO sieht die NIS-Richtlinie in Art. 14 Abs. 3 – im nationalen Recht umgesetzt in § 8b BSGI und § 8c BSIG – eine Meldepflicht von Sicherheitsvorfällen für Betreiber Kritischer Infrastrukturen und Anbieter digitaler Dienste auch dann vor, wenn keine personenbezogenen Daten betroffen sind. Es überrascht wenig, dass die Meldepflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für Betreiber Kritischer Infrastrukturen insoweit am umfangreichsten sind. Letztere haben gem. § 8b Abs. 4 BSIG Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben (Nr. 1) oder führen können (Nr. 2) – d. h. namentlich wie sie durch Cyberangriffe entstehen können – unverzüglich zu melden. Allem voran die Variante des „führen können", § 8b Abs. 4 Nr. 2 ist geeignet, Unternehmen erhebliche Schwierigkeiten zu bereiten. Denn ihnen wird faktisch eine Beurteilung der Gefährdungssituation überlassen, ohne, dass diese für eine anschließende (eigene) Beurteilung durch das BSI bindend ist. Betroffene Unternehmen müssen folglich abwägen, ob der Vorfall einer (möglicherweise mit rufschädigenden Konsequenzen verbundenen) Mitteilung an das BSI bedarf bzw. ob die Gefahr einer Fehleinschätzung zu wahrscheinlich ist, als dass die Nichtmeldung mit einhergehenden Bußgeldern zu riskant ist.

Haftung

Nicht zuletzt aufgrund drohender haftungsrechtlicher Konsequenzen ist eine intensive, umfassende, juristisch fundierte Auseinandersetzung mit Cyberkriminalität angezeigt. Fraglich ist insoweit, welche haftungsrechtlichen Problematiken bzw. Risiken aus zivilrechtlicher, öffentlich-rechtlicher, strafrechtlicher sowie datenschutzrechtlicher Perspektive für die Unternehmen bestehen.

Insoweit droht eine Inanspruchnahme des betroffenen Unternehmens selbst. Zu erwägen ist hier ein schuldrechtlicher Schadensersatzanspruch aus §§ 280 Abs. 1, 2, 286 BGB, wenn beispielsweise Kunden und Lieferanten infolge von Lieferausfällen oder Verzug Datenverluste erleiden.[24] Zudem können Gläubiger möglicherweise unter Berufung auf § 280 Abs. 1 BGB mittels der Rüge einer Verletzung entsprechender Vertraulichkeitspflichten Ansprüche geltend machen.[25] Eine Haftung bei Verletzung von einzelfallabhängigen Sorgfaltspflichten statuiert Art. 82 Abs. 1 DSGVO; eine Norm, die sowohl bei materiellen als auch immateriellen Schäden greift. Allerdings ist die Haftung des Betroffenen dann

18 *Voigt*, IT-Sicherheitsrecht, 1. Aufl. 2018, Rn. 333.

19 *Grages* in Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 33 Rn. 4.

20 *Voigt*, IT-Sicherheitsrecht, 1. Aufl. 2018, Rn. 333.

21 *Voigt/von dem Bussche*, Praktikerhandbuch DSGVO, 1. Aufl. 2018, Teil 3.8.2.2.

22 *Grages* in Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 33 Rn. 7.

23 *Voigt*, IT-Sicherheitsrecht, 1. Aufl. 2018, Rn. 337.

24 *Schmidt-Versteyl*, NJW 2019, 1637, 1638.

25 *Schmidt-Versteyl*, NJW 2019, 1637, 1638.

ausgeschlossen, wenn ihm der Nachweis gelingt, keine Verantwortlichkeit für den Schadenseintritt zu tragen.[26] Eine derartige Exkulpation ist jedoch nur sehr schwer möglich, weshalb das Risiko der Verhängung einer erheblichen Geldstrafe stets einkalkuliert werden muss. Potentielle Schadensersatz- oder Schmerzensgeldansprüche folgen aus §§ 7 und 8 BDSG.

Mit Blick auf die dargestellten Haftungsszenarien ist berechtigterweise zu klären, ob von Seiten des Unternehmens gegen eine drohende Inanspruchnahme nebst den oben bereits dargelegten Maßnahmen weitere Möglichkeiten bestehen, einer Haftung zu entgehen. Entsprechend der Regelung des § 280 Abs. 1 Satz 2 BGB muss das Unternehmen nachweisen können, dass es seinen IT-Sicherheitspflichten ordnungsgemäß und gesetzeskonform nachgekommen ist.[27] Im Umkehrschluss bedeutet das, dass wenn alle erforderlichen Sicherheitsmaßnahmen nachweisbar gewährleistet wurden, das betroffene Unternehmen im Regelfall keine Inanspruchnahme zu befürchten hat. Eine lückenhafte Dokumentation sowie präzise Listung sämtlicher getroffener Sicherheitsmaßnahmen ist folglich mehr als ratsam.

Nicht minder praktisch relevant ist die Frage, wen das betroffene Unternehmen in Anspruch nehmen kann. Allem voran aus finanziellen Gründen. In Betracht kommen hier zunächst Ansprüche gegen den Angreifer selbst. Zivilrechtlich gestaltet sich die Rechtslage wie folgt: Möglich ist ein deliktischer Anspruch gem. § 823 Abs. 2 BGB i.V.m. den seitens des Angreifers im Einzelfall verletzten Schutzgesetzen. Denkbar ist hier insbesondere die Verletzung sämtlicher Straftatbestände mit IT-Relevanz, z.B. § 202a StGB, § 202b StGB, § 263a StGB, § 303a StGB, § 303b StGB oder ergänzend § 17 UWG. Darüber hinaus möglicherweise einschlägig ist § 823 Abs. 1 BGB; konkret in der Variante der Verletzung eines „sonstiges Rechts", speziell eines (betriebsbezogenen) Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb. Sofern die Löschung von Daten zusätzlich die physische Veränderung eines Speichermediums bewirkt, steht dem Unternehmen ggf. ferner ein Anspruch aus § 823 Abs. 1 BGB in der Fallgruppe der Eigentumsverletzung zu. Vertreten wird zudem, dass § 823 Abs. 1 BGB ein eigentumsähnliches "Recht am eigenen Datenbestand" schütze. Bei einem Verstoß gegen das Urheber- oder Markenrecht sind Ansprüche aus § 97 Abs. 2 UrhG sowie § 14 Abs. 6, 7 MarkenG und § 15 Abs. 5, 6 MarkenG zu erwägen. Insoweit können entstandenen Kosten zurückverlangt werden, vorausgesetzt die Identität des Täters ist ermittelbar und der entstandene Schaden ist als ersatzfähiger mittelbarer Schaden anzusehen. Zu beachten ist, dass der Umstand, dass der Angriff aus dem Ausland stattfindet, einer Geltendmachung von Ansprüchen nicht entgegensteht, sofern sich das angegriffene IT-System in Deutschland befindet.

Betreffend möglicher Ansprüche gegen Hilfspersonen des Angreifers ist zwischen vorsätzlichem und fahrlässigem Verhalten der entsprechenden Hilfsperson bzw. deren Unterlassen zu differenzieren. Hat die Hilfsperson den Angreifer vorsätzlich unterstützt, könnte er/sie als Täter oder Teilnehmer nach § 830 BGB zur Verantwortung gezogen werden. Aber auch eine fahrlässige Unterstützung der Tat des Täters iter Umständen haftungsbegründend.[28]

Allerdings erweist sich die Durchsetzung etwaiger Ersatzansprüche in der Praxis erfahrungsgemäß als schwierig. Insbesondere die Identifizierung des Täters / der Täter ist nur selten möglich. Doch selbst bei bekannter Identität stellen die eigentliche Rechtsdurchsetzung sowie die Vollstreckung tatsächliche Probleme dar.[29]

Ass. jur. Lukas Schmidt/Luisa Lorenz

26 *Schmidt-Versteyl*, NJW 2019, 1637, 1638.

27 *Schmidt-Versteyl*, NJW 2019, 1637, 1638.

28 *Mehrbrey/Schreibauer*, MMR 2016, 75 ff.

29 *Schmidt-Versteyl*, NJW 2019, 1637, 1638.

Leiter des Forschungsprojekts und Autoren

Prof. Dr. Dirk Heckmann

Dirk Heckmann studierte Rechtswissenschaften an der Universität Trier. Promotion 1991, Habilitation 1995 an der Universität Freiburg. Er ist seit 1996 Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht und seit 2006 Direktor im Institut für IT-Sicherheit und Sicherheitsrecht an der Universität Passau. Dort leitet er auch die Forschungsstelle für IT-Recht und Netzpolitik For..Net und engagiert sich im DFG-Graduiertenkolleg „Privatheit und Digitalisierung".

2003 wurde er zum nebenamtlichen Verfassungsrichter am Bayerischen Verfassungsgerichtshof gewählt, 2007 in den Expertenkreis des Nationalen IT-Gipfels der Bundesregierung und 2016 in die Ethikkommission des Bundesverkehrsministeriums zum automatisierten und vernetzten Fahren berufen. 2018 folgte die Berufung in die Datenethikkommission der Bundesregierung sowie als Sachverständiger der Nationalen Plattform Zukunft der Mobilität. Im März 2019 wurde Heckmann zum wissenschaftlichen Sprecher der Plattform Verbraucherbelange in der Digitalisierung des Zentrums Digitalisierung Bayern ernannt.

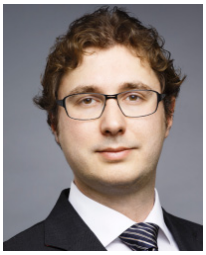
Seit 2014 ist der Internetrechtler Vorsitzender der Deutschen Gesellschaft für Recht und Informatik, seit Oktober 2018 Direktor am Bayerischen Forschungsinstitut für Digitale Transformation in München.

Seine Lehr- und Forschungsschwerpunkte liegen im Schnittfeld von IT und Recht, insbesondere im Datenschutzrecht, IT-Sicherheitsrecht, E-Government, Persönlichkeitsschutz sowie E-Health. Im März 2019 erschien die 13. Auflage des Gola/Heckmann, Kommentar zum Bundesdatenschutzgesetz, im April 2019 folgte die 6. Auflage seines juris Praxiskommentars Internetrecht.

Lukas Schmidt

Lukas Schmidt ist seit Juli 2018 wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau sowie seit Dezember 2018 Kollegiat des DFG-Graduiertenkollegs 1681/2 „Privatheit und Digitalisierung". Das Studium der Rechtswissenschaften hat er 2016 mit der Ersten Juristischen Staatsprüfung in Passau abgeschlossen. Das Referendariat am OLG München hat er 2018 mit der Zweiten Juristischen Staatsprüfung abgeschlossen.

Thomas Schneck



Thomas Schneck ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau. Das Studium der Rechtswissenschaften hat er 2015 mit der Ersten Juristischen Staatsprüfung in Passau abgeschlossen. Das Referendariat am OLG München hat er 2018 mit der Zweiten Juristischen Staatsprüfung abgeschlossen.

Das nächste Magazin erscheint am 15. Dezember 2019. Sie finden das Magazin und die Möglichkeit, sich an- und abzumelden, unter www.baywidi.de

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation

Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung

Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.