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

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur vierten Ausgabe des BayWiDI-Magazins!

Nach einem erfolgreichen Jahr 2019 freue ich mich, die Verlängerung des Projekts bekanntgeben zu dürfen. Das BayWiDI-Angebot wird auch weiterhin ausgebaut und in Zusammenarbeit mit unseren Praxispartnern ab Januar 2020 zu einer gemeinsamen Initiative zusammengeführt werden, die aktuelle Informationen zum Thema Cybersicherheit an die Hand gibt.

Dabei wollen wir uns wie auch bisher besonders von den Bedürfnissen und Interessensschwerpunkten kleiner und mittelständischer Unternehmen leiten lassen. Zu diesem Zweck stehen wir im ständigen Dialog mit Wirtschaft und Wissenschaft und werden auch weiterhin die durch Feedback und Umfragen gewonnenen Erkenntnisse im Kontext der Verlängerung des Projekts in unsere Arbeit einfließen lassen.

In eigener Sache möchte ich Sie darüber hinaus auf das 15. For..Net-Symposium hinweisen, das am 23. und 24. April 2020 unter dem Motto «Gemeinwohl und Digitalisierung» in Passau stattfinden wird; eine ausführliche Ankündigung und Hinweise zur Teilnahme finden Sie nebenan.

In dieser Ausgabe wagen wir einen Rundumschlag: Neben einer allgemeinen Beschreibung der aktuellen Gefährdungslage und der Zusammenfassung der wichtigsten Erkenntnisse des im Oktober veröffentlichten BSI-Berichts zur Lage der IT-Sicherheit in Deutschland 2019 im ersten Beitrag erwartet Sie im zweiten Beitrag eine eingehendere Betrachtung einer der maßgeblichsten Bedrohungen der Cybersicherheit für Behörden, Unternehmen und auch Private, der Ransomware. Beispielhaft werden anhand zweier bekannter Schädlinge die Risiken beleuchtet und anschließend mögliche vorbeugende Maßnahmen

und Reaktionsempfehlungen vorgestellt.

Schließlich finden Sie im dritten Beitrag eine aktuelle Übersicht zu den IT-Sicherheitsrechtlichen Rahmenbedingungen für kleine und mittelständische Unternehmen.

Damit wünsche ich Ihnen eine interessante Lektüre, ein frohes Weihnachtsfest und geruhsame Feiertage sowie einen guten Rutsch in das neue Jahr.

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

Inhalt

15. Internationales For..Net Symposium: »Gemeinwohl und Digitalisierung« am 23. und 24. April 2020

Das 15. Internationale For..Net Symposium widmet sich am 23./24. April 2020 dem Thema „Gemeinwohl und Digitalisierung“. Hochkarätige Referentinnen und Referenten aus Wissenschaft und Praxis beleuchten aus rechtlicher, ethischer, politischer, technischer und ökonomischer Sicht, wie man digitale Technologien und Geschäftsmodelle zum Wohle Aller entwickeln und einsetzen kann. Eröffnet wird die Fachveranstaltung von Valerie Mocker, Direktorin bei der gemeinnützigen britischen Innovationsstiftung NESTA. Sie erhielt im April 2019 den For..Net-Award, einen Preis für herausragende Verdienste um eine gemeinwohlorientierte Digitalisierung. Abgerundet wird das Symposium wie immer durch ein kulturelles und kulinarisches Rahmenprogramm. Nähere Informationen erhalten Sie über https://www.for-net.info/symposien/. Wie schon 2019 wird auch das Symoposium 2020 unterstützt durch das Bayerische Forschungsinstitut für Digitale Transformation (bidt.digital).

Die Lage der IT-Sicherheit in Deutschland 2019

Einleitung

Die Berichte über durch Malware verursachte Schäden sind allgegenwärtig. Das Berliner Kammergericht etwa wird nach einem Angriff mit dem Trojaner Emotet Ende September dieses Jahres erst 2020 wieder am Netz sein. Zwar gelang es der Schadsoftware nicht, Daten abzugreifen und zu verschlüsseln, die IT-Verantwortlichen befürchten allerdings, dass Emotet sich noch im System befinden und schlafend stellen könnte.[1] Auch ausgerechnet das Automatisierungsunternehmen Pilz – als Sicherheitsspezialist für vernetzte Industrie, Schutz derselben vor unbefugten Zugriffen aus dem Netz und Technologien zur optischen und digitalen Überwachung von Industrieanlagen bekannt – wurde Opfer eines Verschlüsselungstrojaners.

Beide Fälle zeigen beispielhaft, dass die IT-Sicherheit in unzähligen Behörden, Unternehmen und anderen Einrichtungen sowie in privaten Netzwerken oft nur unzureichend oder gar nicht gewährleistet ist und teilweise selbst ein sehr verantwortungsbewusster Umgang mit der IT (wie bei Pilz) Angriffe nicht immer zu verhindern vermag.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Cyber-Sicherheitsbehörde des Bundes hat im Oktober einen ausführlichen Lagebericht über die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger und seiner Wirtschaft vorgelegt, in dem die Gefährdungslage näher beleuchtet wird und – mit zahlreichen Beispielen versehen – Angriffsmethoden, aber auch mögliche Lösungsansätze erläutert werden.[2]

Weniger, aber effektivere Angriffe: Cyber-Crime as a Service

Allein 2019 wurden 114 Mio. neue Schadprogramm-Varianten gemeldet. Der Schwerpunkt der Cyber-Angriffe liegt aktuell deutlich im Bereich Cyber-Kriminalität.[3] Besonders besorgniserregend ist die Tendenz zu immer leichter verfügbaren Möglichkeiten für technisch und finanziell weniger leistungsfähige Angreifer, Taktiken und Mittel auf einem Niveau zu nutzen, das vormals bestens ausgestatteten Geheimdiensten vorbehalten war.[4]

E-Mails mit Schadprogrammen zählen dabei zu den am häufigsten detektierten Angriffen auf die Bundesverwaltung[5] und stellen auch für Privatanwender und Unternehmen ein ernstzunehmendes Risiko dar. Meist sind sie ein Einfallstor für weitere Angriffssystematiken und bedrohen hypothetisch (und teilweise auch in der Praxis) jede Person oder Institution, die über eine E-Mail-Adresse verfügt.

Identitätsdiebstahl, Phishing und Spam

Als „Identität" sind in diesem Kontext einzelne oder mehrere Merkmale zu verstehen, die die Echtheit einer Person oder Sache bilden.[6] Identitätsdiebstahl – die rechtswidrige Zueignung solcher Daten – kann etwa mittels Phishing[7] - und Social-Engineering-Methoden verübt werden. Social Engineering bezeichnet Sozialtechniken der Manipulation und Suggestion, die das Opfer dazu bringen, dem Angreifer die gewünschten Informationen freiwillig mitzuteilen.[8] So werden etwa E-Mails verschickt, die legitimen Mails von Banken, Telefonanbietern oder Online-Shops täuschend ähnlich sind, aber einen präparierten Anhang oder Hyperlink enthalten.[9] Ein weiteres bekanntes Beispiel sind betrügerische Support-Anrufe, bei denen sich Kriminelle als Teil des Microsoft-Support-Teams ausgeben und Hilfe bei (vorgetäuschten) Problemen anbieten. Können sie den Angerufenen überzeugen, soll dieser den Zugriff per Fernwartungstool oder Remote Access Tool freigeben; auf diesem Weg kann Schadsoftware auf dem System installiert und damit eine Hintertür für zukünftige Aktivitäten eingerichtet werden.[10] Auch das sogenannte

1 *Krempl*, *Emotet*: Berliner Kammergericht bleibt bis 2020 weitgehend offline, Heise Online, 25.10.2019, abrufbar unter: http://www.heise.de/-4569544, zuletzt abgerufen am 28.10.2019.

2 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (auch ältere Ausgaben), zuletzt abgerufen am 29.10.2019.

3 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7.

4 *Nagel*, BSI warnt: Cyberkriminelle arbeiten inzwischen wie Geheimdienste, Handelsblatt.de, 17.10.2019, abrufbar unter: https://www.handelsblatt.com/politik/deutschland/it-sicherheit-bsi-warnt-cyberkriminelle-arbeiten-inzwischen-wie-geheimdienste/25125986.html?ticket=ST-83185195-4dZXKSmeOYGugiritxbd-ap1, zuletzt abgerufen am 29.10.2019; vgl. auch BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7, 28 f.

5 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 37.

6 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 8.

7 Ausführlich: *Borges*, NJW 2005, 3313.

8 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. 2018, Rn. 333.

9 Vgl. *Kociok* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 27 Rn. 14 ff.

10 *BSI*, Die Lage der IT-Sicherheit in

„Doxing“[11], das die gezielte Recherche nach personenbezogenen Daten und deren anschließende unerlaubte Veröffentlichung im Internet beschreibt, ist ein aktuelles Problem, das eine Vielzahl privater und in der Öffentlichkeit stehender Personen betrifft.[12] Besonders bekannt ist der Fall von Ende 2018, als ein Twitter-User Verlinkungen veröffentlichte, über die der Download umfangreicher Datensammlungen möglich war. Nach dem Vorbild eines Adventskalenders wurde jeden Tag ein „Türchen“ mit neuen privaten Daten von Prominenten und zahlreichen deutschen Politikerinnen und Politikern geöffnet. Unter den Daten befanden sich öffentlich zugängliche Informationen wie dienstliche E-Mail-Adressen, aber auch private Daten und Fotos, die nicht öffentlich einsehbar waren.[13]

Obwohl der Versand von Spam insgesamt und der von Malware-Spam speziell sogar um ca. 97% zurückgegangen ist, ist das Schadpotenzial durch die deutlich gezieltere Versandweise gleichgeblieben und teilweise sogar angestiegen. Auch der Emotet-Befall beim Berliner Kammergericht nutzte E-Mails als Einfalltor.[14] Angreifer zeigen hier ein hohes Maß an Innovation und technischem Sachverstand, sodass in Kombination mit einem erhöhten personellen Aufwand und neuen Social-Engineering-Techniken das Risiko bei Weitem nicht zu vernachlässigen ist. Ein vorsichtiger und restriktiver Umgang mit E-Mail-Anhängen ist hier das Mittel der Wahl, um die Angriffe ins Leere laufen zu lassen.[15]

Malware und Ransomware auf dem Vormarsch

Infektionen durch Schadprogramme wie Trojaner, Viren oder Würmer bleiben wie schon in den Vorjahren eine der größten Bedrohungen für Private, Unternehmen und Behörden und machten im Jahr 2018 einer Umfrage der Allianz für Cyber-Sicherheit zufolge 53% der berichteten Cyber-Sicherheitsvorfälle aus. Als integraler Bestandteil der meisten Angriffsszenarien kann Malware unerwünschte oder schädliche Funktionen auf einem System ausführen; 2019 wurden insgesamt rund 114 Mio. neue Malware-Varianten registriert, von denen über die Hälfte auf Windows-Betriebssysteme entfallen.[16]

Schadsoftware wie der eingangs erwähnte Trojaner Emotet wird seit 2016 vermehrt eingesetzt, um Daten auf dem infizierten System zu verschlüsseln und anschließend Lösegeld (i.d.R. Bitcoin oder andere Kryptowährungen) zu erpressen. Auch häufen sich Berichte, dass die Daten trotz Zahlung des Lösegelds anschließend nicht entschlüsselt werden (können) oder weitere Forderungen gestellt werden.[17]

Für einen vertieften Einblick in das Thema Ransomware-Angriffe und Präventionsmöglichkeiten ist auf die nachfolgende Anmerkung von Jannik Zerbst zu verweisen.

Konstantes Risiko durch DDoS-Attacken und Botnetze

DDoS-Angriffe bezwecken meist nicht das Eindringen in das jeweilige System, sondern dessen Überlastung, etwa um die dabei entstehende Verzögerung für das Einschleusen eigener Antworten zu nutzen (Hijacking) oder parallellaufende Angriffe zu verschleiern bzw. zu ermöglichen.[18] Besonders häufig werden Systeme anvisiert, deren Ausfall für Kundinnen und Kunden deutlich wahrnehmbar ist, beispielsweise Banken oder E-Commerce-Seiten.[19] Das konstant hohe Risiko lässt sich einerseits mit den niedrigschwelligen Angeboten erklären, die selbst für technisch nicht versierte Angreifende zur Verfügung stehen und beruht andererseits auf dem hohen Grad der Konnektivität unterschiedlicher Netzwerke über das Internet und insbesondere über Cloud Services. Serverbasierte Angriffe aus der Cloud sind besonders effizient, da hier sehr schnelle Verbindungen durch die Cloud-Provider zur Verfügung gestellt werden. Teilweise wird die Überlastung auf Anwendungs- und Netzwerkebene kombiniert (Multivektor-Attacken), wogegen ein effektiver Schutz kaum möglich ist; mehr Erfolg versprechen DDoS-Mitigations-Dienstleister, die mittels Künstlicher Intelligenz bereits vor der Anbindung des Betreibers dynamisch Angriffe erkennen und individuelle Maßnahmen zur Bereinigung des Datenstroms einleiten können.[20]

Botnetze bestehen aus automatisierten Computerprogrammen, die von einem Bot-Master kontrolliert werden, um dann beispielsweise Spam- bzw. Phishing-Mails zu verschicken.[21] Mittlerweile werden Botnetze aufgrund der

Deutschland 2019, S. 47.

11 Kunstwort aus „dox“ (documents) und „dropping“, ausführlich: *Kubiciel/Großmann*, NJW 2019, 1050.

12 *Kubiciel/Großmann*, NJW 2019, 1050.

13 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 9.

14 Vgl. *Krempl*, Heise Online, 25.10.2019 (Fn. 1).

15 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 27.

16 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 11.

17 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 16.

18 *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 3 Rn. 271 ff.

19 Insb. zu umsatzstarken Zeitpunkten wie etwa dem Black Friday oder Cyber Monday, vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 18 f., S. 22 f.

20 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 20.

21 *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, 3. Aufl. 2019, § 3 Rn. 270.

zunehmenden kostengünstigeren Alternativangebote (z.B. Booterdienste) seltener für DDoS-Angriffe genutzt, sondern hauptsächlich im Bereich Informationendiebstahl, Betrug beim Onlinebanking sowie zur Verteilung von Malware.[22]

Besonders unter Privaten begründet eine digitale Sorglosigkeit ein ansteigendes Risiko für Botnetz-Infektionen; schon einfache Basismaßnahmen könnten hier Wirkung zeigen. Ein verantwortungsvollerer Umgang seitens der Nutzenden ist jedoch zur Minimierung der Risiken ebenso unerlässlich wie ein IT-Sicherheitsorientierter Ansatz der Hersteller von mobilen Endgeräten und IoT-Systemen. Besonders bei Letzteren muss von Herstellerseite ein höherer Sicherheitsstandard ab Werk implementiert und das System auch mittel- bis langfristig mit Support und Updates versorgt werden. IoT-Infektionen sind zwar infolge der Standardkonfiguration von Routern in Deutschland nicht annähernd so prävalent wie im Ausland; es ist allerdings keineswegs darauf Verlass, dass ein passwortgesicherter Router allein eine Infektion von IoT-Geräten verhüten kann.

APT-Angriffe, Kryptografie und moderne Prozessorarchitektur

Advanced Persistent Threats (APT), die typischerweise auf Angreifende mit staatlicher Förderung hinweisen, stützen sich immer häufiger auf die Verwendung öffentlich verfügbarer Penetrationstest-Werkzeuge, die in ihrer Funktionalität mit Spionageprogrammen vergleichbar sind. Da insbesondere unerfahrene Kriminelle oft Voreinstellungen nutzen, können Logdaten und Netzwerkverkehr jedoch entsprechend gezielt gescannt werden. Versiertere Angreifende hingegen entwickeln ihr eigenes Schadprogramm-Arsenal weiter. Berichten von IT-Sicherheitsfirmen zufolge soll es auf internationaler Ebene eine zunehmende Anzahl von Dienstleistern geben, die Spähsoftware und Exploits anbieten oder sogar selbst Cyber-Angriffe operativ durchführen. So ist es auch Staaten mit bisher geringem Know-How möglich, hochprofessionelle Angriffswerkzeuge zu besitzen und zu nutzen.[23] Auch legitime Dienste wie etwa Dropbox, Google Groups oder Github werden verwendet, was hinsichtlich der Präventionsmaßnahmen zu einem hohen organisatorischen Aufwand für Sicherheitsteams führt und darüber hinaus Aspekte des Datenschutzes berührt. Dennoch können viele APT-Angriffe durch gängige IT-Sicherheitsmaßnahmen verhindert werden.[24]

Im Zusammenhang mit Verschlüsselungsverfahren ergeben sich vorwiegend dann Risiken für Cyber-Angriffe, wenn das System nicht ordnungsgemäß implementiert und abgesichert wurde, zu schwache Zufallszahlen verwendet werden oder Seitenkanäle sowie kryptografische Mechanismen und Protokolle nicht ausreichend stark und gesichert sind. Genau in diesen Punkten ist bei der Verbesserung des Schutzes durch Verschlüsselungstechniken anzusetzen.[25]

Moderne Prozessoren führen Code teilweise spekulativ anhand entsprechender Vorhersagen aus. Ergebnisse aus falschen Vorhersagen oder unberechtigten Zugriffen werden zwar transient ausgeführt (d.h. sie werden verworfen und nicht weitergegeben), allerdings ist die hierbei anfallende Änderung des mikroachitekturellen Zustands der CPU (etwa des Cache-Inhalts) unter bestimmten Voraussetzungen von Angreifern wahrnehmbar und kann so mittelbar zur Offenlegung geschützter Inhalte führen. Allerdings spielen Angriffe, für die die Prozessorarchitektur des zu infiltrierenden Systems ausgenutzt werden, eine eher untergeordnete Rolle und betreffen eher konkrete einzelne Ziele als die breite Masse.[26]

22 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S.21.

23 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 28.

24 Vgl. die Empfehlungen des BSI unter https://www.bsi.fuer.buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/Basisschutz Geraet_node.html, zuletzt abgerufen am 29.10.2019.

25 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 30.

26 *BSI*, Die Lage der IT-Sicherheit in

Lösungsansätze und Empfehlungen des BSI

Hinsichtlich der steigenden Fälle von Identitätsdiebstahl und der immer gezielteren Taktik von Angreifenden, mithilfe von Social Engineering Zugang zu Systemen zu erlangen, ist ein noch intensiverer Schutz digitaler (privater) Identitäten und persönlicher Daten ein absolutes Muss. Auch die eigenständige Veröffentlichung potenziell sensibler Informationen sollte dringend dem Gebot der Datensparsamkeit folgen. Da allerdings nur eine einzige Schwachstelle erfolgreich ausgenutzt werden muss, um ein System zu infiltrieren, stellt sich Cyber-Sicherheit asymmetrisch dar. Nötig ist also eine möglichst ganzheitliche Betrachtung der Faktoren Technik – Organisation – Mensch.[27] Bei größeren Unternehmen und solchen aus der IT-Branche sind ein größeres Bewusstsein und dem folgend auch umfassendere Sicherheitsmanagementsysteme (ISMS) vorhanden. Dagegen verfügen unter den befragten kleinen und mittelständischen Unternehmen nur knapp 40% über ein Notfallmanagement, ein zentrales Patch-Management bzw. ein ganzheitlich ausgelegtes ISMS.

Allgemein nennt das BSI (neben technischen Lösungen) Sensibilisierung und Eigenverantwortung im Umgang mit der Digitalisierung als notwendige Antworten auf den zunehmenden Missbrauch digitaler Identitäten.[28] Konkret kann – beispielsweise nach Common Criteria (ISO/IEC 15408) oder nach den Technischen Richtlinien oder dem IT-Grundschutzkatalog des BSI – ein möglichst umfassendes Sicherheitsmanagement implementiert und zertifiziert werden.[29]

Fazit

Angriffe auf IT-Systeme sind infolge der fortschreitenden Vernetzung verschiedenster Systeme über das Internet immer verbreiteter, dank Cybercrime-as-a-service[30] und ständig überarbeiteten Schadprogrammen mit Versionsnummer und Patches zunehmend organisierter und im Hinblick auf die Masse der online (frei oder durch Datenleaks und -hacks) verfügbaren persönlichen Informationen deutlich gezielter als in der Vergangenheit.

Oft fehlt es bereits an grundlegenden Basismaßnahmen: Auf den inzwischen vom Netz genommenen Rechnern des Kammergerichts läuft beispielsweise – Stand 31. Oktober – noch immer ein hoffnungslos veraltetes System, das auf Windows 95 basiert und dessen Abschaffung schon 2017 dringendst gefordert wurde.[31] Dabei ist ein aktuelles System, das regelmäßig mit Updates und Patches versorgt wird, einer der Grundpfeiler für Cyber-Sicherheit, sowohl für die private Nutzung als auch für Unternehmen und Behörden.

Zusammenfassend lässt sich daher feststellen: Das Schutzniveau kann auf institutioneller Ebene noch so hoch und das ISMS noch so ausgefeilt sein – das nach wie vor größte IT-Sicherheitsrisiko sitzt vor dem Bildschirm.

Die wirkungsvollste Prävention lässt sich daher grundsätzlich durch konsequente Weiterbildung und Schulungen, einen kritischen Umgang mit E-Mail-Anhängen und Links sowie ein aktuell gehaltenes System erreichen. Etwaige Schäden können durch regelmäßige und umfassende Backups minimiert werden.

Priska Katharina Büttel

Deutschland 2019, S. 32 f.

27 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 46 ff.

28 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7.

29 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 52.

30 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 20.

31 *Kiesel/Keilani*, IT-Katastrophe am Berliner Kammergericht kam mit Ansage, Tagesspiegel, 29.10.2019, abrufbar unter: https://amp.tagesspiegel.de/berlin/experten-warnten-schon-2017-it-katastrophe-am-berliner-kammergericht-kam-mit-ansage/25163810.html, zuletzt abgerufen am 30.10.2019.

Ransomware – Funktion, Angriffsvektoren und Schutz

Im Lagebericht des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit in Deutschland 2019 wird der Einsatz sog. Ransomware als eines der maßgeblichsten Bedrohungsszenarien, insbesondere auch für deutsche Unternehmen, beschrieben.[1] Aufgrund dieser vom BSI beschriebenen Aktualität des Themas, aber auch weil unter Ransomware zu fassende Angriffsszenarien hohe Schäden für Unternehmen verursachen können, widmet sich dieser Beitrag sowohl der Beschreibung der Funktionsweise von Ransomware und den bekannten Bedrohungsszenarien als auch den Schutzmöglichkeiten bzw. Reaktionsempfehlungen.

Was ist Ransomware und wie funktioniert sie?

Ransomware, eine erpresserische Malware, stellt einen Teil aus dem Potpourri internetbasierter Angriffe dar.[2] Ransomware beschreibt im Grunde nur als Kunstbegriff eine bestimmte Einsatzform von Malware.[3] Hierbei handelt es sich grundsätzlich um eingesetzte Schadsoftware, die zum Eindringen auf fremde Rechner genutzt wird, diese infiziert und (meist) die auf der lokalen Festplatte gespeicherten Daten verschlüsselt, um die berechtigten Nutzerinnen und Nutzer vom Zugang zu den Daten auszuschließen. Für die Entschlüsselung dieser Daten wird anschließend eine Lösegeldsumme gefordert.[4] Die Verschlüsselung von Daten ist letztlich auf jedem Endgerät denkbar.[5] Bei dem Begriff Ransomware handelt es sich daher um die Zusammensetzung aus Malware (eingesetzte **Schadsoftware**) und Ransom (Forderung einer **Lösegeldsumme**). Wo Eckert noch 2014 die Zahlung der Lösegeldsummen via Online-Zahlungssysteme wie mitunter PayPal als besonders häufige Forderung feststellte[6], gibt das BSI hingegen im aktuellen IT-Sicherheitslagebericht die Begleichung erpresster Summen mittels Kryptowährung als die 2018/2019 meist genutzte Methode an.[7]

Mitunter weite Bekanntheit hat das Thema Ransomware mit den WannaCry-Angriffen im Jahr 2017 erreicht. Publik wurden die Angriffe mit dem Fall des britischen nationalen Gesundheitssystems, bei dem innerhalb eines kurzen Zeitraums eine Vielzahl von Einrichtungen Opfer dieser Ransomware wurden.[8] Besonders betroffen waren ältere Windows-Versionen, welche nicht mehr hinreichend mit Updates versorgt wurden.[9] Der Angriff auf die englischen Krankenhäuser hatte zur Folge, dass mehrere Patientinnen und Patienten, die teils auch wegen Krebs- und Herzerkrankungen behandelt wurden, aufgrund der fehlenden Datensätze in andere Kliniken verlegt werden mussten oder nach Hause geschickt wurden.[10] Schon vor der Möglichkeit einer Lösegeldzahlung war also bereits ein nicht unerheblicher Schaden eingetreten. In Deutschland etwa hatte WannaCry die Systeme der Deutschen Bahn angegriffen und letztlich zu der Aufnahme von Ermittlungen durch das Bundeskriminalamt geführt.[11]

Welche Bedrohungsszenarien sind bekannt?

Von Ransomware-Angriffen sehen sich Privatpersonen genauso bedroht wie Unternehmen, Behörden und Krankenhäuser.[12] Nach den Feststellungen des BSI sind Ransomware-Angriffe nach Meldungen aus der Wirtschaft im Jahr 2019 weiterhin zentral.[13] Die Zielgruppen von Ransomware-Angriffen können Opfer verschiedener Angriffsvektoren werden:[14]

1 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7, 25ff. abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 23.10.2019.

2 *Eckert*, IT-Sicherheit, De Gruyter, 2014, S. 24.

3 *Eckert*, IT-Sicherheit, De Gruyter, 2014, S. 24.

4 *Eckert*, IT-Sicherheit, De Gruyter, 2014, S. 24.

5 *Ehmann* (Hrsg.), Lexikon für das IT-Recht 2019, 9. Aufl. 2019, S. 71.

6 *Eckert*, IT-Sicherheit, De Gruyter, 2014, S. 24.

7 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 16.

8 *Briegleb*, heise, https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html, zuletzt abgerufen am 25.10.2019.

9 *Briegleb*, heise, https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html, zuletzt abgerufen am 25.10.2019.

10 *Briegleb*, heise, https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html, zuletzt abgerufen am 25.10.2019.

11 *Heise*, https://www.heise.de/newsticker/meldung/WannaCry-BKA-ueber-nimmt-Ermittlungen-nach-weltweiter-Cyber-Attacke-3713467.html, zuletzt abgerufen am 25.10.2019.

12 *Ehmann* (Hrsg.), Lexikon für das IT-Recht 2019, 9. Aufl. 2019, S. 71.

13 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 47.

14 *BSI*, Die Lage der IT-Sicherheit in

- (a) Eine Infiltration der Systeme mit der die Daten verschlüsselnden Schadsoftware kann über Spam-E-Mails stattfinden. Die Malware kann sich entweder im Anhang der E-Mail befinden oder über eine URL verlinkt sein.

- (b) Bei sog. „Drive-by-Exploits“ werden Schwachstellen von Browsern, Browser-Plug-Ins oder Betriebssystemen ausgenutzt. Hierbei findet eine Infizierung über den Aufruf von kompromittierten Webseiten oder darauf platzierter Werbung statt.

- (c) Täter können unter Verwendung von „Exploit-Kits“, also einer Zusammenstellung verschiedener Systemschwachstellen, gezielt durch eine vorbestimmte Angriffsart und Übertragungsweise der Schadsoftware Angriffe starten.

Der BSI-Lagebericht beschreibt auch, dass darüberhinausgehend Unternehmen Opfer von Ransomware-Attacken werden können, indem etwa schwache Passwortsicherungen oder Schwachstellen in Fernwartungs-Werkzeugen ausgenutzt werden.[15] Hat ein Schadprogramm die ersten Hürden überwunden, können Schwachstellen eines Betriebssystems zur Verschleierung der Bösartigkeit der Software genutzt werden.[16]

Das israelische Sicherheitsunternehmen Votiro Secured wies bereits Ende vergangenen Jahres darauf hin, dass gerade im Bereich der Ransomware-Kriminalität nicht zwingend die groß angelegten Angriffs-Kampagnen oder besonders komplexen Programme zu fürchten seien, sondern insbesondere die Tatsache, dass zunehmend im Dark Web Ransomware-Anwendungen erworben und genutzt werden können, also allein die Menge der zu erwartenden Codes, die sich jeweils in ihrer Art der Kodierung voneinander unterscheiden, zunimmt.[17] Noch dazu handelt es sich bei

diesen low-level-Ransomware-Varianten um besonders kostengünstig zu erwerbende Software, die Einsatzschwelle wird demzufolge weiterhin sinken.[18]

Beispielhaft sollen die Ransomware-Varianten **SamSam** und **Ryuk** genauer beschrieben werden:

SamSam

SamSam ist eine Variante aktiverer Ransomware,[19] die sich bisher überwiegend auf den US-amerikanischen Bereich konzentriert hat, deren Nutzung in weiteren Ländern jedoch nicht zwingend auszuschließen ist. Einige Nutzungen haben bereits stattgefunden.[20] Anders als der Großteil von Ransomware werden als Angriffsvektoren gerade keine Phishing-Kampagnen oder Exploit-Kits genutzt. Beim Einsatz von SamSam werden vielmehr gezielt Server kompromittiert und als Ausgangspunkt für weitere Angriffe auf zu einem Netzwerk verbundene Systeme genutzt.[21]

Zugriff auf die Server wird überwiegend im Wege der sog. Brute-Force-Attacken[22] oder unter Nutzung gestohlener Zugangsdaten erlangt.[23] Auf diese Weise kann der initiale Zugriff auf die Serversysteme durchaus schwer aufzudecken sein, weil dieser letztlich über einen erlaubten Zugang stattfindet.[24] Hat der Zugriff auf die Server stattgefunden, greifen die Kriminellen unter anderem weitere Zugangsdaten und Administratorrechte ab und gelangen so in die Position, weitere Malware auf die verbundenen Systeme nachzuladen, ohne dass weitere Schritte durch einzelne Nutzer (etwa das Öffnen eines E-Mail-Links) erforderlich sind.[25]

Nachdem die Angreifenden sich die gewünschten Daten verschafft und diese verschlüsselt haben, fordern sie ihre Opfer über Nachrichten, die sie auf den verschlüsselten Computern hinterlassen, dazu auf, über vorgegebene Kanäle Kontakt aufzunehmen und die Begleichung der geforderten Lösegeldsumme durchzuführen.[26] Nachdem die Opfer die Lösegeldsumme (meist durch Zahlung von Bitcoins) beglichen haben, erhalten diese oftmals (jedoch nicht in al-

Deutschland 2019, S. 17, auch im Folgenden.

15 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 17.

16 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 17.

17 Votiro, https://votiro.com/how-hackers-will-think-in-2019-low-hanging-fruit-and-sophistication-in-future-cyber-attacks/, zuletzt abgerufen am 25.10.2019.

18 Votiro, https://votiro.com/how-hackers-will-think-in-2019-low-hanging-fruit-and-sophistication-in-future-cyber-attacks/, zuletzt abgerufen am 25.10.2019.

19 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 17.

20 CISA USA, https://www.us-cert.gov/about-us, zuletzt abgerufen am 25.10.2019.

21 Cisco, https://blogs.cisco.com/security/talos/samsam-the-doctor-will-see-you-after-he-pays-the-ransom, zuletzt abgerufen am 24.10.2019.

22 Methode, um Passwörter durch automatisiertes, wahlloses Ausprobieren zu erraten, vgl. *Luber/Schmitz*, Security Insider, https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/, zuletzt abgerufen am 25.10.2019.

23 CISA USA, https://www.us-cert.gov/about-us, zuletzt abgerufen am 25.10.2019.

24 CISA USA, https://www.us-cert.gov/about-us, zuletzt abgerufen am 25.10.2019.

25 CISA USA, https://www.us-cert.gov/about-us, zuletzt abgerufen am 25.10.2019.

26 CISA USA, https://www.us-cert.gov/about-us, zuletzt abgerufen am 25.10.2019.

len Fällen) über einen Link die richtigen Schlüssel und Werkzeuge zugeschickt, mit denen sie die Verschlüsselung der Daten rückgängig machen können.[27]

Ryuk

Anfang dieses Jahres vermeldete das Nachrichtenportal Spiegel-Online, dass die Ransomware-Variante Ryuk in Deutschland Einzug gefunden hat.[28] Der Befall mit dieser weiterhin aktiven[29] Verschlüsselungssoftware findet in mehreren Schritten statt. Die Verschlüsselungssoftware selbst wird erst über den Trojaner Emotet[30] bzw. über die Schadsoftware TrickBot auf die bereits infizierten Systeme nachgeladen.[31]

Emotet wird den Betroffenen meist via Spam-Mail zugespielt und fungiert hierbei als Türöffner für die Infizierung des Systems mit einer weiteren Schadsoftware namens TrickBot.[32] Dieses Programm wiederum ist in der Lage, unter anderem Kontozugangsdaten der Betroffenen auszuspähen, um den Angreifern einen Überblick über die möglichweise erpressbaren Lösegeldsummen zu bieten.[33] TrickBot lädt dann die eigentliche Ransomware Ryuk nach, welche für die Verschlüsselung der (im Rahmen der Auskundschaftung des Systems als wichtig erkannten) Daten sorgt.[34] Hat die Verschlüsselung der Daten stattgefunden, kann die eigentliche Erpressung stattfinden. Hierbei werden regelmäßig außerordentlich hohe Summen gefordert, was sich gerade bei Unternehmen, die sich längere „Offline"-Zeiten nicht leisten können, als besonders rentabel darzustellen scheint.[35] Ryuk unterscheidet sich in der Angriffsmethode und Vorgehensweise von sonst üblichen Ransomware-Angriffen dahingehend, dass hier konkret gezielte Angriffe durchgeführt werden, die mitunter derart designt sind, dass sich auch kleinere Operationen profitabel durchführen lassen.[36]

Schutzmöglichkeiten

Das Internetportal „nomoreransom.org", das zur Unterstützung von Opfern von Ransomware-Angriffen gegründet wurde, sieht für die Wiedererlangung der Kontrolle über die verschlüsselten Daten ohne die Zahlung der geforderten Lösegeldsumme grundsätzlich nur geringe Erfolgsaussichten.[37] Der Prävention von Ransomware-Angriffen hingegen werden vergleichsweise höhere Erfolgschancen zugeschrieben.

So empfiehlt das IT-Sicherheitsunternehmen SOPHOS im Hinblick auf die oben beschriebene Ransomware Ryuk etwa die Schulung von Personal und jedem, der das System nutzt, die Verwendung starker Passwörter, die Kontrolle von Zugangsrechten, Backups der Systeme vorzuhalten, ein geeignetes Patch-Management zu betreiben und insbesondere Anti-Ransomware-Software einzusetzen.[38]

27 CISA USA, https://www.us-cert.gov/about-us, zuletzt abgerufen am 25.10.2019.

28 *Beuth*, Spiegel Online, https://www.spiegel.de/netzwelt/web/ransomware-ryuk-so-erpressen-kriminelle-grosse-unternehmen-a-1248112.html, zuletzt abgerufen am 25.10.2019.

29 Vgl. *Adam*, Sophos News, Beitrag vom 4.10.2019, https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/, zuletzt abgerufen am 25.10.2019.

30 Vgl. BayWiDI Aktuelles, *Jannik Zerbst*, 30.01.2019.

31 *Adam*, Sophos News, https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/, zuletzt abgerufen am 25.10.2019.

32 *Beuth*, Spiegel Online, https://www.spiegel.de/netzwelt/web/ransomware-ryuk-so-erpressen-kriminelle-grosse-unternehmen-a-1248112.html, zuletzt abgerufen am 25.10.2019.

33 *Beuth*, Spiegel Online, https://www.spiegel.de/netzwelt/web/ransomware-ryuk-so-erpressen-kriminelle-grosse-unternehmen-a-1248112.html, zuletzt abgerufen am 25.10.2019.

34 *Beuth*, Spiegel Online, https://www.spiegel.de/netzwelt/web/ransomware-ryuk-so-erpressen-kriminelle-grosse-unternehmen-a-1248112.html, zuletzt abgerufen am 25.10.2019.

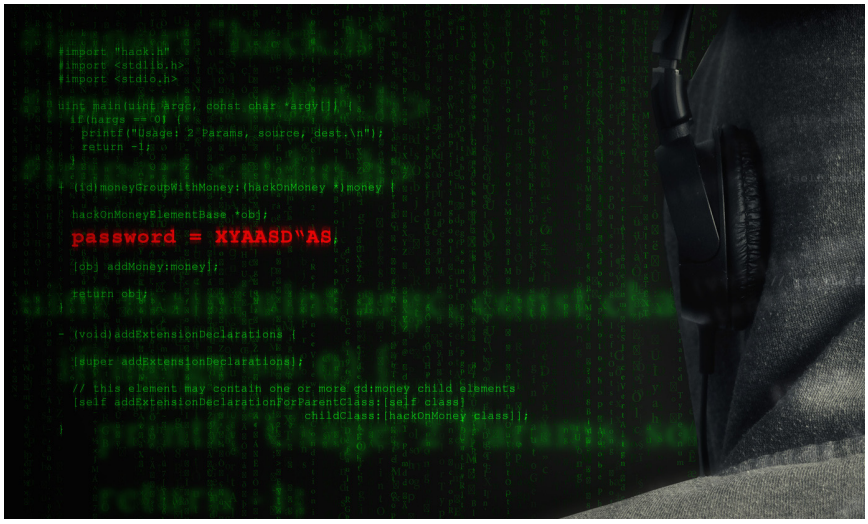
35 *Adam*, Sophos News, https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/, zuletzt abgerufen am 25.10.2019.

36 *Cohen/Herzog*, CheckPoint Research, https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/, zuletzt abgerufen am 25.10.2019.

37 Nomoreransom, https://www.nomoreransom.org/de/index.html, zuletzt abgerufen am 24.10.2019.

38 *Adam*, Sophos News, https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/, zuletzt abgerufen am 25.10.2019.

Es lassen sich hinsichtlich Angriffsvorbeugung und Methodik der Ransomware-Angriffe **zwei Gruppen** unterteilen, die gleichermaßen in ein funktionierendes IT-Sicherheitskonzept einzubeziehen sind. Sowohl die technischen Systeme eines Unternehmens als auch die dort beschäftigten Personen, also der Faktor Mensch, können Schwachstellen bieten, die sich durch Angreifende ausnutzen lassen.



IT-Sicherheitsstruktur

Grundlegend empfiehlt das BSI zur Vorbeugung von Ransomware-Angriffen, für regelmäßige Backups der Systeme, zumindest der besonders wichtigen Dateien, zu sorgen. Darüber hinaus sollten Unternehmen die Angriffsfläche für Virusattacken möglichst weit reduzieren, etwa indem nur begrenzt von außen auf Rechner zugegriffen werden kann.[39] Da Ransomware-Angriffe zunächst nichts anderes sind als der Befall mit Schadsoftware, finden die allgemeinen Sicherheitsvorkehrungen Anwendung. Unter anderem regelmäßige Updates und insbesondere auch zeitnahe Aktualisierungen der Betriebssysteme sind dabei unerlässlich.[40]

Faktor Mensch

Dem Faktor Mensch, gem. dem Bundeskriminalamt oft das „schwächste Glied der Sicherheitskette“[41], kann bereits dadurch begegnet werden, dass die Gruppe derjenigen Personen, die auch über das Internet auf die IT-Systeme eines Unternehmens zugreifen können, eher gering gehalten wird.[42] Wie oben erwähnt helfen darüber hinaus auch Schulungen des Personals über den richtigen Umgang mit IT-Systemen und den existierenden Bedrohungsvarianten der Cyberkriminalität. Hierüber lassen sich Sicherheitslücken, die sich über sogenanntes Social Engineering[43] ausnutzen lassen, minimieren. Zur sicheren Nutzung der Systeme zählt dann mitunter auch die Einrichtung starker Passwörter,[44] hierzu sollten die Beschäftigten eines Unternehmens demzufolge besonders angehalten werden.

Was tun, wenn ein Angriff stattfindet bzw. stattgefunden hat?

Auch wenn das Unternehmen eine gute Schutzstruktur gegen Ransomware-Übergriffe vorhält, lassen sich erfolgreiche Angriffe nicht mit absoluter Sicherheit ausschließen. Im Falle eines gelungenen Angriffs mit Ransomware werden sich gerade solche Unternehmen, die längere Offline-Zeiten hohe Geldsummen kosten, schnell zur Zahlung der geforderten Lösegeldsummen verleiten lassen. Im Frühling dieses Jahres etwa verweigerte ein norwegischer Konzern die Zahlung einer Lösegeldsumme und machte durch den gesperrten Zugang zu wichtigen Daten bereits in der ersten Woche einen Verlust in Höhe von etwa 40 Millionen Euro.[45] Nach Angaben des BSI stellt das Begleichen der Lösegeldzahlung dennoch in vielen Fällen keine vielversprechendere Alternative dar. Teilweise ist es den Opfern von Ransomware-Angriffen auch nach Zahlung der erpressten Gelder nicht möglich, die verschlüsselten Daten oder blockierten Zugänge wiederherzustellen, weil die Täter die hierfür benötigten Schlüssel nicht preisgaben, gar nicht mehr reagierten oder sogar weitere Lösegeldzahlungen verlangten.[46] Die Behörde empfiehlt daher auch grundsätzlich, von der Zahlung eines Lösegeldes abzusehen.[47]

Handelt es sich um ältere oder bereits bekannte Varianten von Schadprogrammen, so sind hierfür teilweise bereits Entschlüsselungstools vorhanden und werden etwa auf der Ransomware-Bekämpfungsseite nomoreransom.org frei zur Verfügung gestellt.[48]

Jannik Zerbst, LL.M. (VUW)

39 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 18.

40 Avast, https://www.avast.com/de-de/c-ransomware, zuletzt abgerufen am 30.10.2019; BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 18.

41 Bundeskriminalamt (BKA), https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html, zuletzt abgerufen am 30.10.2019, unter „Datendiebstahl durch Social Engineering“.

42 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 18.

43 Hierbei wird gezielt auf telefonischem, elektronischem oder gar persönlichem Weg der Kontakt zum Menschen gesucht, um an Passwörter oder wichtige Daten zu gelangen. Im Zuge dessen wird oftmals ein Vertrauensverhältnis zum Opfer hergestellt und Sympathie kreiert, um anschließend an sensible Informationen des potenziell Geschädigten zu gelangen, vgl. BKA, https://www.bka.de/DE/Service/FAQs/SocialEngineering/socialEngineering_node.html;jsessionid=F20DC9462432ED775B629BC34C473DF1.live0611, zuletzt abgerufen am 30.10.2019, unter „Was ist Social Engineering?“.

44 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 18.

45 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 17.

46 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 17.

47 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 18.

48 Siehe hierzu: https://www.nomoreransom.org/de/decryption-tools.html, zuletzt abgerufen am 30.10.2019.

IT-Sicherheitsrechtliche Rahmenbedingungen für KMU in Deutschland

Einleitung

Kleine und mittelständische Unternehmen (KMU) bilden in Deutschland den sog. Mittelstand, soweit 99, 3 % der deutschen Unternehmen als KMU zu klassifizieren sind.[1] In der Rolle als Arbeitgeber und Arbeitgeberin der breiten Masse sowie Motor für das BIP ist die Bedeutung von KMU in Deutschland – wie allseits bekannt – nicht zu unterschätzen. Aus diesem Grunde ist auch die Frage der Rechtssicherheit für diese Gruppe von Unternehmen von elementarer Bedeutung für das wirtschaftliche Gefüge in Deutschland. Doch nicht nur die Sicherheit in rechtlicher Hinsicht, sondern auch die Sicherheit mit Blick auf die Handhabung der IT, die einem Unternehmen zur Verfügung steht, spielt seit Jahren eine immer größer werdende Rolle.[2]

Das IT-Sicherheitsrecht soll den Unternehmen dabei eine Richtschnur sein, um die beiden genannten Risikofelder der Rechtsunsicherheit und der „IT-Unsicherheit" zu vermeiden. Dabei mag es jedoch fast ironisch anmuten, dass der regulatorische Rahmen, der für Deutschland maßgeblich durch europäisches und nationales Recht geprägt wird, zumindest in der Fläche – bis jetzt – nicht durch eine breite Rahmengesetzgebung geprägt ist, sondern überwiegend aus einem Flickenteppich normgeprägter Ansätze besteht.

Dieser Artikel versucht – wie viele andere auch[3] – nun diesen Flickenteppich zusammenzutragen. Soweit ersichtlich ist die rechtswissenschaftliche Literatur dabei meist[4] darauf bedacht, lediglich die Normen und ihre Rechtsfolgen in abstrakter Weise wiederzugeben. Dieser Text soll versuchen, einen Mittelweg zwischen der Auflistung eines „Normenwaldes" und einer reinen „Praxis-Checkliste" abzubilden.

Diesem Muster entsprechend werden im weiteren Verlauf zunächst noch einmal zur Klarstellung die hier verwendeten Begriffe der KMU und des IT-Sicherheitsrechts definiert. Im Anschluss erfolgt die Darstellung der gesetzlichen Einfallstore für die gesetzlichen Rahmenbedingungen der IT-Sicherheit von KMU in Deutschland. Bei der Betrachtung bleiben die Aspekte des Datenschutzes allerdings außen vor, soweit diese bereits in vorangegangenen Texten ausführlich thematisiert wurden.[5] Danach erfolgen konkrete Hinweise für die unternehmerische Praxis.

Definitionen

Zunächst gilt es aber, KMU und das IT-Sicherheitsrecht zu definieren. Die Europäische Kommission definiert KMU, für die Zwecke ihrer Regularien in Anlehnung an die etablierte Praxis, als Unternehmen mit einer Mitarbeiterzahl von bis zu 250 und einem Jahresumsatz von nicht mehr als 50 Millionen Euro oder einer Jahresbilanz von nicht mehr als 43 Millionen Euro.[6]

Schwieriger ist schon die Definition des IT-Sicherheitsrechts als solches. Passend zum verteilten regulatorischen Rahmen gab es auch lange Zeit keine einheitliche Definition der IT-Sicherheit.[7] In Anlehnung an den in diesem Kontext stets bemühten § 2 BSIG definiert die rechtswissenschaftliche Literatur die IT-Sicherheit nun aber ersichtlich einheitlich als dasjenige, das gewährleistet ist, „wenn die in einem informationstechnischen System hinterlegten Informationen verfügbar sind, und zwar einschränkend immer dann, wenn dies erforderlich (und vereinbart) ist [Verfügbarkeit], für jeden Nutzer, der hierzu berechtigt ist (und dies nachweist), und zwar nur für diesen [Vertraulichkeit] und mit genau dem Inhalt, den der Urheber geschaffen hat [Integrität]. Zusätzlich müssen die Informationen jedem Urheber in dem Maße zurechenbar sein, in dem der Zweck der Informationsverarbeitung diese Zurechnung fordert [Authentizität oder Prüfbarkeit]"[8]. Diese durch das BSIG vorgegebene Definition wird dabei stets durch den Zusatz der Authentizität, der gelegentlich auch als Prüf-

1 *Statistisches Bundesamt*, „Verteilung der Unternehmen in Deutschland nach Unternehmensgröße im Jahr 2017 [Graph]" vom 24. Oktober, 2019, abgerufen über: Statista, von https://de.statista.com/statistik/daten/studie/731901/umfrage/verteilung-unternehmen-in-deutschland-nach-unternehmensgroesse/, zuletzt abgerufen am 20.11.2019.

2 Nach einer Umfrage von Bitkom gaben 68% der befragten 503 Unternehmen mit mehr als 20 Mitarbeiter/-innen im Jahr 2018 an, von Datendiebstahl, Industriespionage oder Sabotage betroffen gewesen zu sein. 19% gaben an, vermutlich betroffen zu sein (vgl. Bitkom, „War Ihr Unternehmen in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen?", abgerufen über: Statista, von https://de.statista.com/statistik/daten/studie/150885/umfrage/anteil-der-unternehmen-die-opfer-von-digitalen-angriffen-wurden/, zuletzt abgerufen am 20.11.2019).

3 Vgl. dazu exemplarisch: *Heckmann*, MMR 2006, 280 ff. oder Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019

4 Zu Ausnahmen vgl. etwa: *Schmidl*, NJW 2010, 476 ff. sowie *Trappehl/Schmidl*, NZA 2009, 985 ff.

5 Vgl. dazu etwa *Scheurer/Walker*, „IT-Sicherheit. Privat? – Grund- und datenschutzrechtliche Aspekte einer privaten Pflicht zur IT-Sicherheit", BayWiDI-Magazin März 2019, S. 9 ff.; Zerbst, „WhatsApp-Nutzung in Unternehmen", BayWiDI-Magazin Juni 2019, S. 8 ff.

6 Vgl. *Eurostat*, https://ec.europa.eu/eurostat/de/web/structural-business-statistics/structural-business-statistics/sme, zuletzt aufgerufen am 20.11.2019.

7 Vgl. etwa den Hinweis von *Schmidl*, NJW 2010, 467 (477).

8 *Heckmann*, in: jurisPK Internetrecht, 4. Aufl. 2014, Kapitel 5 Rn. 219.

barkeit[9] umschrieben wird, ergänzt.[10]

Verfügbarkeit meint dabei primär die Erhaltung der Zugangsmöglichkeit zur jeweiligen IT (bspw. über regelmäßige Back-Ups),[11] während die Vertraulichkeit gerade sicherstellt, dass der Zugang nur der berechtigten Person gegenüber erfolgt (bspw. über die Nutzung einer Ende-zu-Ende-Verschlüsselung),[12] oder Anonymisierungsverfahren über „hashen" bzw. „salzen").[13] Die Integrität umfasst die Erhaltung der IT in ihrer jeweils konkret gewünschten Form ohne Verfälschungen (bspw. auch über die Verwendung von Verschlüsselungen oder Hardware-Firewalls i.V.m. einem Intranet),[14] und die Authentizität sichert die Zurechenbarkeit von Personen und ihren Interaktionen mit der IT (bspw. über die Verwendung von Signaturen bei der Ende-zu-Ende-Verschlüsselung).[15]

Das Recht hat nun die Aufgabe, diese Kernprinzipien in ihrer Entfaltung zu gewährleisten und die dabei auftretenden Zielkonflikte[16] auszutarieren oder zumindest Wege zu ebnen, auf denen die relevanten Parteien dies selbst vornehmen können.

Der konkrete Rechtsrahmen und seine Folgen

Dies erfolgt dabei über die nahezu gesamte Bandbreite an regulatorischen Möglichkeiten: vom größtenteils den Parteien in der Gestaltung überlassenen zivilrechtlichen Privatrecht, über konkreten Vorgaben in Spezialgesetzen wie dem TMG, bis hin zur ultima ratio des Strafrechts.

Dabei bietet das geltende Recht also nicht einen Ansatzpunkt, sondern viele einzelne Einfallstore, die aber auf eine Verpflichtung hindeuten: nämlich die grundlegende Implementierung eines Risikomanagements zur Etablierung von präventiven und bereinigenden Maßnahmen mit Blick auf IT-Sicherheitsproblemlagen im einzelnen Unternehmen.

Einfallstor TMG

So sind nach § 13 Abs. 7 des TMG[17] grundsätzlich alle KMU, die ein Multimedia-Angebot über bspw. Websites oder Apps anbieten, dazu verpflichtet, durch technische Maßnahmen zu verhindern, dass ein unbefugter Zugang zu diesen Angeboten gestattet wird. Ebenso besteht eine Verpflichtung zum Schutz des störungsfreien Betriebsablaufs. Unsicherheiten ergeben sich dabei in gewisser Weise durch die Orientierung am Stand der Technik, welcher nach der ständigen höchstrichterlichen Rechtsprechung nicht zwingend mit dem geltenden Wirtschaftsstandard gleichzusetzen ist.[18]

Einfallstor Gesellschaftsrecht

Überdies gilt seit dem Inkrafttreten des KonTraG eine Konkretisierung hinsichtlich der Pflichten der Geschäftsleitung.[19] Jedenfalls ab diesem Zeitpunkt war klar: IT-Sicherheit ist Chef und Chefinnen-Sache. Zwar wurde durch das KonTraG maßgeblich nur der § 91 Abs. 2 AktG eingefügt, durch welchen alle Vorstandsmitglieder dazu verpflichtet werden, im Rahmen der gewissenhaften Geschäftsführung i.S.d. § 93 Abs. 1 S. 1 AktG ein Überwachungssystem zu etablieren, dass zur Früherkennung derjenigen Entwicklungen führt, die den Bestand der Aktiengesellschaft gefährden.[20] Dazu gehört nach dem KonTraG auch die Erkennung und Vermeidung von IT-Risiken.[21] Die Einhaltung dieser Anforderungen an den Vorstand ist vom Aufsichtsrat gem. §§ 111 Abs. 1, 76 f. AktG zu überwachen.

Die Maßnahmen zur Erkennung und Vermeidung von IT-Risiken sind nach § 317 Abs. 4 HGB ebenfalls im Jahresabschlussbericht niederzulegen, was gem. § 317 Abs. 2 HGB durch einen Abschlussprüfer kontrolliert wird.[22]

Diese Pflichten gelten jedoch nicht nur für die Aktiengesellschaft, sondern auch für alle sonstigen Formen der Kapitalgesellschaften auf Basis allgemeiner Prinzipien.[23] Insoweit wird durchaus eine Breitenwirkung über die Einbeziehung der GmbH, KG, OHG erzeugt, soweit die letzten beiden zumindest dann den Kapitalgesellschaften gleichgestellt werden, wenn keine natürlichen Personen als persönlich Haftende vorhanden sind.[24]

Allerdings ist anzumerken, dass nicht jedes IT-Risiko den Bestand der Gesell-

9 Vgl. *Schmidl*, NJW 2010, 467 (477).

10 *Heckmann*, MMR 2006, 280 (282).

11 *Conrad*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 9.

12 Auch wenn Meta-Daten (wie eine Absender- oder Absenderinnen-Adresse) hierbei teils noch unverschlüsselt bleiben.

13 *Conrad*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 9.

14 Vgl. *Heckmann*, MMR 2006, 280 (281), der den Begriff der Unversehrtheit verwendet.

15 *Heckmann*, MMR 2006, 280 (282).

16 Beispielsweise zwischen der Vertraulichkeit und der Authentizität.

17 Dessen Geltung im Rahmen der Anwendung der DSGVO zwar streitig, aber wohl anzunehmen ist, soweit es sich nicht um personenbezogene Daten handelt; vgl. dazu *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 300.

18 Vgl. etwa BGHZ 181, 253 = NJW 2009, 2952.

19 *Trappehl/Schmidl*, NZA 2009, 985 (985 f.).

20 *Trappehl/Schmidl*, NZA 2009, 985 (986).

21 Jedenfalls aufgrund faktischer Notwendigkeit; so auch *Heckmann*, MMR 2006, 280 (282).

22 *Grünendahl/Steinbacher/Will*, „Das IT-Gesetz: Compliance in der IT-Sicherheit", S. 2.

23 Trappehl/Schmidl, NZA 2009, 985 (986).

24 Trappehl/Schmidl, NZA 2009, 985 (986).

schaft gefährdet, sodass nicht zwingend für jeden Fall ein Überwachungssystem eingerichtet werden muss. Jedoch sind gerade die Auswirkungen von IT-Risiken auf den Gesellschaftsbestand im Vorhinein nicht immer klar zu bestimmen. Insoweit bestünde jedenfalls ein Haftungsrisiko für die Gesellschaft oder deren Vorstandsmitglieder im Falle der bewussten Eröffnung von Lücken im Überwachungssystem. In jedem Fall lässt das KonTraG aber auch offen, wie genau das Überwachungssystem zu implementieren ist und welchen Anforderungen es genügen muss.[25]

Einfallstor Vertragsrecht

Ebenso fließt die IT-Sicherheit im Rahmen von vertraglichen Pflichtverletzungen ein. So kann etwa die Erbringung der vertraglich zugesicherten Leistung durch Störungen im Betriebsablauf ausgelöst durch Soft- oder Hardwareprobleme zu einer eigenen Haftung des Unternehmens oder der Unternehmensführung führen. Selbiges gilt in Fällen, in denen Kunden und Kundinnen Zugriff auf die eigene IT-Infrastruktur gewährt wird oder schlicht eine E-Mail mit schadhaften Anhängen weitergeleitet wird. Je nach Organisationsgrad können hierbei im Einzelfall zwar externe IT-Sicherheits-Anbieter und Anbieterinnen oder auch interne Mitarbeiter und Mitarbeiterinnen in Regress genommen werden,[26] jedoch müssen sich die Regressnehmenden ggf. ein eigenes Mitverschulden auf Basis einer fehlerhaft eingerichteten Organisationsstruktur oder Kontrolle derer nach § 254 BGB anrechnen lassen, sodass der Regress hier geringer ausfallen kann als die eigene Haftung.

Unsicherheiten ergeben sich insoweit, als dass hier stets ein fahrlässiges Verhalten der potenziell haftenden Person i.S.d. § 276 BGB gefordert wird, dass zudem grundsätzlich zu Lasten dieser Person vermutet wird (vgl. § 280 Abs. 1 S. 2 BGB). Insoweit trifft das Unternehmen oder die Unternehmensführung der Entlastungsbeweis. Um diesen zu führen, bedarf es einer klar nachweisbaren Struktur für die Organisation der IT-Sicherheit. Die Unsicherheiten ergeben sich dadurch, dass die erforderlichen Maßnahmen unter dem Vorbehalt des technisch Möglichen[27] sowie wirtschaftlich Zumutbaren stehen.[28]

Einfallstor deliktische Haftung

Überdies kann das IT-Sicherheitsrecht bei einer gesetzlichen Haftung nach dem Deliktsrecht i.S.d. § 823 Abs. 1, Abs. 2 und § 831 Abs. 1 BGB sowie dem Produkthaftungs- wie Produktsicherheitsgesetz eine Rolle spielen. Bei § 823 Abs. 1 BGB ist dabei insbesondere die Verletzung von Verkehrssicherungspflichten relevant, die aus der mangelnden Kontrolle der eigenen IT-Infrastruktur abgeleitet werden kann. Jedoch trifft die geschädigte Person hierbei die Beweispflicht hinsichtlich der Verletzung einer solchen Verkehrssicherungspflicht, welche im Regelfall nicht zu erfüllen sein wird, sodass das Haftungsrisiko an dieser Stelle geringer ausfällt.[29]

Etwas Anderes mag im Falle von Herstellern von Produkten oder produktgebundenen Dienstleistungen gelten, bei denen im Rahmen der von der Rspr. entwickelten sog. Produzentenhaftung eine Beweislastumkehr zugunsten der Betroffenen stattfindet, sodass die Pflichtverletzung zumindest zunächst nicht mehr nachgewiesen werden muss.[30] Jedoch muss der oder die Betroffene dann immer noch die Kausalität zwischen der Pflichtverletzung und der Schädigung nachweisen, was dadurch bedingt, dass grundsätzlich mehrere verschiedene IT-Produkte und -Dienstleistungen häufig gemeinsam verwendet werden, schwer zu bewältigen sein wird.[31]

Selbiges gilt für eine Haftung aus § 823 Abs. 2 i.V.m. Spezialgesetzen wie §§ 203 Abs. 1, 13 Abs. 1 StGB sowie § 831 Abs. 1 BGB, die zumeist indirekt ebenfalls an die Verletzung einer Verkehrssicherungspflicht anknüpfen, deren Nachweis für Außenstehende schwer zu führen sein wird.

Außerdem ist im Falle dieser Haftungstatbestände zu beachten, dass diese grundsätzlich keine reinen Vermögensschädigungen erfassen, was eine weitere Hürde darstellt.[32] Aus denselben Gründen spielt meist auch das Produkthaftungs- sowie das Produktsicherheitsgesetz keine Rolle, bei denen ohnehin zweifelhaft ist, ob sie auf reine Softwarelösungen Anwendung finden.[33]

25 *Speichert*, Praxis des IT-Rechts, 2. Aufl. 2007, 9.2.4, S. 250.

26 Wobei dieser bei internen Mitarbeitern und Mitarbeiterinnen durch den innerbetrieblichen Schadensausgleich meist geringer ausfallen dürfte als die dem Unternehmen oder der Unternehmensführung auferlegte Haftung.

27 Insoweit ist darauf hinzuweisen, dass die Rspr. hier nicht die „best-practice"-Standards genügen lässt, sondern regelmäßig auf den jeweiligen Stand der Technik verweist, vgl. etwa. BGHZ 181, 253 = NJW 2009, 2952.

28 Vgl. für die Vorgaben in § 13 Abs. 7 TMG *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 300.

29 *Spindler*, MMR 2008, 7 (9).

30 *Spindler*, MMR 2008, 7 (9).

31 *Spindler*, MMR 2008, 7 (9).

32 *Spindler*, MMR 2008, 7 (9).

33 Auch wenn die wohl h.M. dies bejaht, fehlt es an einer höchstrichterlichen Rechtsprechung, vgl. *Mankowski*, in: Ernst (Hrsg.), Hacker, Cracker & Computerviren, 2004, Rn. 441; *Marly*, Softwareüberlassungsverträge, 4. Aufl. 2004, Rn. 1303; Sodtalbers, Softwarehaftung im Internet, 2006, Rn. 161; *Koch*, Versicherbarkeit von IT-Risiken, 2005, Rn. 607.

Dennoch besteht ein – wenn auch geringes – Haftungsrisiko an dieser Stelle.

Einfallstor positive Diskriminierung

Überdies bietet die Einhaltung von IT-Sicherheit Ansätze für positive Diskriminierungen. So kann im Vergaberecht sowohl im Rahmen der Leistungsbeschreibung als auch bei der Bewertung von Angeboten bei der Vergabe öffentlicher Aufträge ein Auge auf die IT-Sicherheit des Unternehmens geworfen werden.[34]

Auch Versicherungen machen ihre Angebote, bedingt durch die Verpflichtungen über Solvency II, von der Einhaltung der IT-Sicherheitsstandards abhängig.[35] Selbiges gilt auf Basis von Basel II und III auch bei Banken im Rahmen ihrer Kreditvergabe an Unternehmen.[36]

Einfallstor Gewerbe- und Wettbewerbsrecht

Zudem bleibt die Gefahr, dass Unternehmen bei Vernachlässigung der IT-Sicherheit das Betreiben eines Gewerbes gem. § 35 GewO auf Basis der Unzuverlässigkeit untersagt wird oder Behörden allgemeine Auflagen erteilen.[37]

Im Wettbewerbsrecht ist das Risiko der Abmahnung durch Konkurrenten und Konkrentinnen, aber auch die Gefahr der Haftung bei der Werbung mit IT-Sicherheit und Nichteinhaltung dieser versprochenen Standards nach § 9 UWG gegeben.

Einfallstor Straf- und Ordnungswidrigkeitenrecht

Ebenfalls ergeben sich konkrete Straftatbestände, wie der § 203 StGB oder § 106 UrhG, und Ordnungswidrigkeiten, wie im § 16 Abs. 2 Nr. 3 TMG oder § 130 OWiG.

Grundrechtliche Grenzen der IT-Sicherheit

Jedoch bleiben insbesondere aus grundrechtlicher Perspektive, die im Zivilrecht zumindest mittelbar zur Geltung kommt, auch Grenzen für diese Einfallstore. So gilt es im Unternehmen auch das Fernmeldegeheimnis gem. Art. 10 GG zu Gunsten der Mitarbeiter und Mitarbeiterinnen zu schützen. Ergänzt wird dies durch das allgemeine Persönlichkeitsrecht und – daraus abgeleitet – insbesondere durch den Schutz der Vertraulichkeit und der Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Relevant wird dies insbesondere bei technischen Überwachungsmaßnahmen gegenüber den Mitarbeitern und Mitarbeiterinnen mit Blick auf die Spam-Filterung von E-Mails[38] oder die Verwendung eigener Endgeräte.

Insoweit besteht zwar ein rechtlicher Rahmen, doch bleiben viele Fragen offen, soweit sich Haftungsmaßstäbe und rechtliche Vorgaben an einem Stand der Technik innerhalb des wirtschaftlich Zumutbaren orientieren und keine Angaben dazu machen, wie dieser Weg beschritten werden soll. Die Benennung eines „Safe Harbour“ für KMU fällt dadurch grundsätzlich schwer. Hilfreich können jedoch die Angaben des BSI sein, das von staatlicher Seite beauftragt ist, gerade auch KMU bei der Implementierung von IT-Sicherheitsstandards zu unterstützen und auch jenes zu zertifizieren.[39]

Es gilt hierbei zu beachten, dass gerade bei KMU die grundsätzliche „Awareness“ mit Blick auf IT-Sicherheit besteht, es jedoch zumeist an Personal und nötigen finanziellen Mitteln fehlt, um die notwendigen Maßnahmen nachhaltig umzusetzen.[40] Im Endeffekt läuft es damit auf die Etablierung eines Risikomanagement-Systems hinaus, welches hilft, die getroffenen Maßnahmen des Unternehmens aufzuzeichnen und die Abwägungsprozesse zwischen technisch Notwendigem und wirtschaftlich Zumutbarem darzulegen, sodass auch eine einfachere gerichtliche Nachprüfbarkeit besteht.

Damit leiten sich folgende Maßstäbe aus der Praxis der Compliance ab: So sind zunächst die Risiken im Unternehmen selbst zu identifizieren; dabei gibt es keine schematische Lösung, sondern nur einen am einzelnen Unternehmensmodell orientierten Ansatz. Hierbei gilt es, alle Prozessabläufe des Unternehmens zu „mappen“, um die relevanten Akteure und Akteurinnen, ihre Beziehung untereinander und die jeweiligen Schnittstellen zu verwendeter IT zu überprüfen und auf Einzelrisiken zu prüfen. Hilfreich ist dabei die Untergliederung der Problembereiche in menschliches Handeln und technische bzw. organisatorische Mängel.

Bei menschlichem Handeln ergeben sich vor allem Probleme durch einfache Nachlässigkeiten, wie beim Herunterladen externer Software oder dem Öffnen von externen E-Mail-Anhängen sowie dem

34 *Heckmann*, MMR 2006, 280 (283 f.).

35 *Hupertz/Conrad*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, Rn. 353 f.

36 *Hupertz/Conrad*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, Rn. 340 ff.

37 *Heckmann*, MMR 2006, 280 (283 f.).

38 Vgl. dazu BVerfG, NJW 2009, 2431 auf das Schmidl verweist in NJW 2010, 476 (479 f.).

39 Vgl. https://www.bsi.bund.de/DE/Themen/StandardsKriterien/standardskriterien_node.html, zuletzt abgerufen am 21.11.2019 und https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html, zuletzt abgerufen am 21.11.2019.

40 Vgl. *BSI*, „Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen – Grad der Sensibilisierung des Mittelstandes in Deutschland“, 2011, S. 8.

Herunterladen externer E-Mail-Inhalte (bspw. Bildelemente), der Verwendung dezentraler Speichergeräte (wie USB-Sticks) und der Duldung, dass Mitarbeitende eigene Geräte nutzen. All dies wird auch begünstigt durch die menschliche Psyche und deren Anfälligkeit für Social Engineering, dessen Einsatz derzeit vermehrt zum Erfolg von KI[41]-gestützten Spam-Mail-Generatoren führt.[42]

Im Rahmen technischer Mängel stellt sich die gegenwärtige Problemlage insbesondere hinsichtlich der Nutzung veralteter Software oder Hardware dar, die durch ausbleibende Serviceleistungen der Anbieter nicht mehr auf den neuesten Stand gebracht werden können, sodass ewige Sicherheitslücken bestehen. Zusätzlich fehlt es häufig an internen Netzwerken, die – abgesichert durch Hardware-Firewalls – die Erkennung externer Zugriffe erschweren. In Anbetracht eines regelrechten Marktes für Schadsoftware im Darknet ist dies eine sehr große Gefahr.[43]

Blickt man auf die organisatorischen Mängel, so kann festgestellt werden, dass es meist noch an klaren Strukturen für die Handhabung der menschlichen wie technischen Fehler mangelt. Es braucht hierbei ein klares Planungskonzept, um die Aufgabenverteilung festzuhalten, Mitarbeiter und Mitarbeiterinnen-Schulungen, die über bloße allgemeine Informationshinweise hinausgehen, sowie interne Meldesysteme der verwendeten Technik und gerade der Reaktion in Notfällen.

Nach der Identifizierung der Risikofaktoren und deren Zuordnung zu konkreten Stellen im Betriebsablauf erfolgt eine Definition von Richtlinien, die Maßnahmen enthalten, um die gesichteten Risiken zu vermeiden und effektives Handeln in den Fällen zu ermöglichen, in denen sich die Risiken dennoch realisiert haben. Dabei gilt es, konkrete Abwägungen zwischen der zu gewährleistenden Sicherheit, dem reibungslosen Angebot der Produkte und Dienstleistungen sowie dem wirtschaftlich Machbaren zu treffen. Hilfreich können dabei die von *Dieffal* aufgestellten Kriterien[44] sein, sowie ein Vergleich zu den jeweils branchenüblichen Standards[45]. Zwar werden durch diese Standards nach der Rechtsprechung des BGH nicht zwingend Haftungen ausgeschlossen, soweit man sich am Stand der Technik zu orientieren hat. Doch geht es eben auch nicht um die schematische Übernahme eines Standards, sondern um die Beschreibung des Abwägungsprozesses im konkreten Einzelfall für oder gegen eine Maßnahme unter Zuhilfenahme der Standards, um Unternehmensentscheidungen im Ernstfall für Gerichte transparent und nachvollziehbar zu machen. Soweit die jeweiligen Entscheidungen auf dieser Basis logisch nachvollziehbar und gut begründet sind, ist eine Haftung in den meisten Fällen auszuschließen.

Daraus abgeleitet ergibt sich ein konkretes Schutzkonzept, dass es umzusetzen gilt. Wesentliche Bestandteile müssen die Verteilung klarer Zuständigkeiten und Zugriffsrechte, die Festlegung technischer Standards an den jeweiligen Schnittstellen, ein Notfallplan, die Nutzung von Kontrollmechanismen[46] sowie die regelmäßige Revision des gesamten Konzepts sein.

Etablieren KMU diese Maßnahmen, wird so nicht nur eine potenzielle Haftung oder Sanktionierung ausgeschlossen, sondern es eröffnet sich auch die Möglichkeit, nachhaltige Rufschädigungen in ein gewinnbringendes Werbekonzept der IT-Sicherheit umzumünzen.

Zusammenfassung

So ist schließlich festzuhalten, dass das IT-Sicherheitsrecht nach über 30 Jahren noch immer einem Flickenteppich gleicht. Wünschenswert wäre ein IT-Sicherheitsrecht 2.0, das – ähnlich der Diskussion zum für KMU ebenfalls essentiellen Lieferkettengesetz – ein Rahmengesetz mit konkreten Pflichtbeschreibungen bietet, die über Öffnungsklauseln in andere Gesetze, wie die Gewerbeordnung oder das TMG, einwirken können. In der jetzigen Debatte über das kommende IT-Sicherheitsrecht 2.0 ist dies noch nicht vollständig absehbar.

In der Praxis wurde versucht, dieses Problem durch breit zugängliche Compliance-Lösungen auszugleichen. Eine Orientierung an diesen Standards wird bei konkreter, nicht schematisierter Anwendung auf das jeweilige Unternehmen dabei auch grundsätzlich eine etwaige Haftung oder Sanktionierung ausschließen und eröffnet die Möglichkeit, das Unternehmensimage um einen weiteren „Asset“ zu erweitern, soweit sich die Umsetzung der IT-Sicherheit nicht in der planerischen Theorie erschöpft.

Til Bußmann-Welsch

41 Im Sinne von „schwacher“ KI.

42 *Andreas May*, Oberstaatsanwalt beim ZIT in seinem Referentenbeitrag auf dem Anwaltszukunftskongress 2019.

43 *Bachmann/Arslan*, NZWiST 2019, 241 (243).

44 Vgl. dazu *Dieffal*, MMR 2015, 716 (718).

45 Vgl. dazu https://www.bsi.bund.de/DE/Themen/StandardsKriterien/standards-kriterien_node.html, zuletzt abgerufen am 21.11.2019.

46 Bei mangelnder Kontrolle und Durchsetzung bestünde andernfalls auch die Problematik der Bildung einer betrieblichen Übung, die sich als rechtlich standhafter Gegensatz zum Compliance-System des Unternehmens etablieren kann. Vgl. dazu *Trappehl/Schmidl*, NZA 2009, 985 (988).

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 folgt die 6. Auflage seines juris Praxiskommentars Internetrecht.

Priska Katharina Büttel

Priska Katharina Büttel hat Anfang 2019 ihr Erstes Juristisches Staatsexamen in Passau abgeschlossen. Seit Oktober 2019 ist sie geschäftsführende wissenschaftliche Mitarbeiterin der Forschungsstelle für IT-Recht und Netzpolitik (For..Net) an der Universität Passau und arbeitet an ihrer Promotion.

Jannik Zerbst, LL.M. (VUW)

Jannik Zerbst ist seit Januar 2018 wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau. Das Studium der Rechtswissenschaften hat er 2016 mit der Ersten Juristischen Staatsprüfung in Passau abgeschlossen. Er promoviert gegenwärtig zu Rechtsfragen im Rahmen der Digitalisierung von Bibliotheks- und Archivbeständen.

Til Bußmann-Welsch

Seit November 2019 ist Til Martin Bußmann-Welsch Wissenschaftlicher Mitarbeiter an der Forschungsstelle für IT-Recht und Netzpolitik (For..Net).

Er hat sein Erstes Juristisches Staatsexamen Ende 2019 in Berlin abgeschlossen und arbeitet zudem als Wissenschaftlicher Mitarbeiter bei Herrn Prof. Dr. Breidenbach.

Das nächste Magazin erscheint am 15. März 2020.
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.