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

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur zweiten Ausgabe des BayWiDI-Magazins.

14. Internationales For..Net Symposium „Digitale Bildung. Digitale Haltung“

Bereits zum vierzehnten Mal jährte sich das Internationale For..Net Symposium in Passau und stand dieses Jahr unter dem Thema „Digitale Bildung. Digitale Haltung“. Als Leiter der Forschungsstelle For..Net, konnte ich auch dieses Jahr unter der Schirmherrschaft der Staatsministerin für Digitales, MdB *Dorothee Bär* am 25. und 26.4.2019 bekannte Referentinnen und Referenten in die Redoutensäle in Passau laden. Hierbei wurden aktuelle Entwicklungen im Rahmen des Themas aus politischer, juristischer und gesellschaftlicher Sicht diskutiert und ethisch beleuchtet. Im Rahmen des feierlichen Abendprogramms auf der Veste Oberhaus wurde *Valerie Mocker* für ihr eminentes gesellschaftliches Engagement der For..Net Award 2019 verliehen. *Mocker* ist ein Vorbild für das „Geschäftsmodell Gemeinwohl“: sie ebnet Innovationen auf dem Gebiet der Digitalisierung den Weg, auch wenn diese ansonsten keine Förderung erhalten würden. Der Preis wurde dieses Jahr gestiftet von der Juris GmbH. Weitere Informationen zum Ablauf, dem Inhalt und den Highlights der Veranstaltung können Sie dem folgenden Tagungsbericht entnehmen, der Ihnen einen prägnanten Überblick hierüber liefert.

In der zweiten 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 „IT-Sicherheitsgesetz 2.0: verlässliche Sicherheit durch zertifizierte Kennzeichnung?“ wird die geplante Neu

fassung des IT-Sicherheitsgesetzes unter dem Gesichtspunkt des angedachten IT-Sicherheitskennzeichens kritisch dargestellt und analysiert. Das geplante Kennzeichen soll den Verwendern technischer Produkte einen belastbaren Überblick über das bestehende Sicherheitsniveau des jeweiligen Produkts verschaffen. Der Beitrag erläutert die geplante Funktionsweise, setzt sich mit den zu erwartenden Vor- und Nachteilen auseinander, wirft einen Blick auf die europäischen Regelungsstrukturen und zieht ein Fazit bzgl. der praktischen Auswirkungen.

Der zweite Beitrag mit dem Titel „WhatsApp-Nutzung im Unternehmen“ setzt sich mit dem juristisch bisher nur wenig erforschtem Phänomen WhatsApp und ähnlichen Kommunikationsmitteln auseinander und beantwortet die Frage, aus welchen Gründen deren Einsatz sowohl unternehmensintern, als auch zur Kommunikation mit dem Kunden problematisch sein könnte.

Der dritte Beitrag mit dem Titel „Malvertising – Gefahr durch Online-Werbung“ beschäftigt sich mit den Gefahren für die IT-Sicherheit eines Unternehmens, die sich aus schädlicher Online-Werbung ergeben können. Hierzu wird zu Beginn der Begriff des „Malvertising“ definiert und dessen verschiedene Erscheinungsformen dargestellt. Daraufhin werden dem Leser mehrere Sicherheitsmaßnahmen an die Hand gegeben, um sich vor einer Infektion durch „Malvertising“ zu schützen.

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

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

Inhalt

- Tagungsbericht 14. Internationales For..Net Symposium / 2
- IT-Sicherheitsgesetz 2.0: verlässliche Sicherheit durch zertifizierte Kennzeichnung? / 5
- WhatsApp-Nutzung im Unternehmen / 8
- Malvertising – Gefahr durch Online-Werbung / 11
- Leiter des Forschungsprojekts und Autoren / 13
- Impressum / 13

Tagungsbericht 14. Internationales Symposium der Forschungsstelle für IT-Recht und Netzpolitik (For..Net) „Digitale Bildung. Digitale Haltung“ am 25. und 26.4.2019 in Passau

Das vierzehnte Internationale For..Net-Symposium in Passau widmete sich in diesem Jahr dem Thema „Digitale Bildung. Digitale Haltung“.

Bei der Begrüßung verwies die Präsidentin der Universität Passau, *Prof. Dr. Carola Jungwirth,* anlässlich des 40-jährigen Jubiläums der Universität besonders auf deren fakultätsübergreifende Grundlagenforschung zu den Auswirkungen der Digitalisierung und der Umsetzung innovativer Konzepte.

Prof. Dr. Dirk Heckmann hält die Begrüßgunsrede in der Redoute (© Robert Geisler)

Das For..Net-Symposium fand erstmals in Kooperation mit dem Bayerischen Forschungsinstitut für Digitale Transformation (bidt) statt, in dessen Direktorium der Leiter der Forschungsstelle For..Net *Prof. Dr. Dirk Heckmann* berufen wurde. Zudem wurde das Saarland als erstes Partnerland 2019 ernannt.

Unter anderem aufgrund dessen wurde die Veranstaltung mit der Verlesung eines Grußwortes von *Ammar Alkassar*, dem Bevollmächtigten für Innovationen und Strategien des Saarlandes, eröffnet. *Alkassar* betonte, dass mit der Beschleunigung der Wandlungsprozesse in der Bildung die Notwendigkeit entstehe, der jungen Generation die erforderlichen Fähigkeiten zu vermitteln, um mit eben diesen Wandlungsprozessen umgehen zu können. Insbesondere digitale Bildung sei dabei von entscheidender Bedeutung und Tragweite.

Ähnlich äußerte sich Schirmherrin MdB *Dorothee Bär* in einer zugeschalteten Videobotschaft, indem sie das Individuum als den Mittelpunkt der digitalen Bildung bezeichnete, da in sämtlichen Fach- und Alltagsbereichen vor allem die Werte der einzelnen Menschen von Bedeutung seien. Ihre „Think outside the box“-Gedanken repräsentierte auch *Bärs* Miniatur eines Flugtaxi-Prototypen. Sie plädierte dafür, national den Gründergeist zu erwecken.

Sodann sprach *Prof. Dr. Ursula Münch*, Direktorin der Akademie für Politische Bildung in Tutzingen, die Keynote „Digitale Bildung als Aufgabe der politischen Gestaltung“ und machte die Wichtigkeit des Fragenstellens deutlich, welches sodann zu Diskussionen verleiten würden. Hinsichtlich des Begriffs „Digitale Bildung“ kritisierte *Münch*, dass dieser oft als technisches Werkzeug degradiert würde, unsere Perspektiven sich jedoch ändern und wir nicht mit sondern in der digitalen Welt arbeiten müssten. Da nicht nur junge Menschen digitale Medien anwende, sollten diese als sog. „Digital Natives“ nicht mehr im Fokus stehen als jeder Anwender. *Münch* erläuterte auch, dass es in der Bildung wichtig sei, die Digitalisierung voranzubringen, indem z.B. die Bildungshoheiten der Länder ausgeglichen und Lehrkräfte aus- und fortgebildet werden. Es benötige einer generationsübergreifenden Aufgeschlossenheit bezüglich der digitalen Fortbildung und ihrer Sinnfrage.

Die Gründerin und Geschäftsführerin der acs plus GmbH, *Christin Schäfer*, hob hervor, dass nur eine auch *sinnvolle* Nutzung der Technik entscheidend ist. Die digitale (Nutzungs-)Kompetenz erfordere das Verständnis, grundlegende technische Strukturen zu lernen, aber vor allem den Willen zum Lernen. Sie verglich den Aspekt des Mitdenkens und Verstehens mit dem Stand in der Medizin im Jahr 1350: Die Digitalisierung sei momentan nicht greifbar, daher könne die klassische evolutionäre Lernstrategie nicht funktionieren. *Schäfer* sprach sich für einen aktiven Kommunikationsaustausch aus und warnte auch vor den Gefahren in der digitalen Welt, die durch die dort herrschende vollständige Ablösung entstünden. Daher sei eine bewusste Herangehensweise unverzichtbar, besonders mit Blick auf Art. 2 GG. Jeder Einzelne sei für sich selbst und seine Sicherheit verantwortlich und dürfe sich nicht auf andere verlassen, weshalb digitale Kompetenzen für jedermann notwendig wären. Ein „One fits it all“-Konzept lehnte *Schäfer* ausdrücklich ab.

Ganz im Zeichen des Kernthemas widmete sich *Prof. Dr. Dirk Heckmann* der „Digitale[n] Bildung als rechtliche Herausforderung“ und stellte sich der Frage nach einem Grundrecht auf digitale Bildung, welches aufgrund der potentiellen Grundrechtsgefährdung mangels ausreichender individueller Fähigkeiten, Kenntnisse und Fertigkeiten sowie aufgrund fehlenden Bewusstseins bezüglich drohender Folgen der Digitalisierung zu erwägen sei. Zumindest begründe Art. 26 der Menschenrechtserklärung der Vereinten Nationen das Recht eines Jeden auf Bildung. Fraglich sei nur, ob dies auch ein Recht auf digitale Bildung umfasse. *Heckmann* gliederte den Begriff der digitalen Bildung in einer Trias aus Methoden, Inhalten und Organisation. Von den Modernisierungsansätzen des E-Governments-Gesetzes, sind Schulen nach Art. 1 Abs. 2 BayEGovG mitinbegriffen und nehmen daher nicht in gleichem Maße teil. Strategisch gesehen müsste aber gerade im Bereich der

Bildung digitale Transformation eingebracht werden und dies möglichst zeitnah, da sich die aktuellen Standards nahe der unteren Grenzen befänden. Dennoch räumte der Referent ein, dass im Zuge der Digitalisierung aus Haftungsgründen vor allem dem Datenschutz und einer dementsprechenden Erziehung hierzu, eine hohe Bedeutung zukäme. Um dies zu verdeutlichen, zitierte er Datenschutzfragen aus dem Schulalltag, vgl. Art. 85 BayEUG.

Prof. Dr. Mario Martini, Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Hochschule Speyer, fokussierte sich in seinem Vortrag auf die politischen Chancen des nationalen Bildungsregisters und dessen rechtliche Grenzen. Problematisch sei dieses insbesondere im Hinblick auf datenschutz- und kompetenzrechtliche Aspekte. Ausgehend von der ausschließlichen Gesetzgebungskompetenz des Bundes bezeichnete *Martini* Bildung als durch die Länder kreiertes Mosaik, bei dem der Bund nur vereinzelte Steine gestalten dürfte. Somit führe das Grundgesetz zu einem Bildungsstatistikvertrag. Ein Bildungsregister könnte sich als Meilenstein erweisen, um das Fundament für Bildungsentscheidungen zu legen und das Datenschutzrecht zu beachten.

Anschließend referierte *Ann Catrin Riedel*, Vorsitzende des LOAD e.V. sowie Mitglied der AG Ethik der Initiative D21 zum Thema „Bildung und Digitalpolitik: Wo bleibt die Zivilgesellschaft?“. *Riedel* zeigte auf, dass Digitalisierung uns Reflexion über das Ausmaß des Auslebens unserer Werte gebe. In Anbetracht aktueller gesellschaftlicher Thematiken, wie der „Fridays for Future“-Bewegung betonte *Riedel*, wie wichtig eine zeitnahe, die „breite Masse“ ansprechende Verbreitung der digitalen Bildung wäre. Die Zivilbevölkerung müsse Digitalisierung in den Alltag integrieren und dürfte nicht auf die Freiheitsgarantie für künftige Generationen vertrauen. Vielmehr müsse das Bewusstsein bezüglich eigener Rechte und deren Verteidigung gestärkt werden.

In der anschließenden Podiumsdiskussion zum Thema „Digitale Bildung, Digitale Haltung: was nun zu tun ist!“ wurde der von *Riedel* zuvor aufgeworfene Impulsgedanke – wo denn die Zivilgesellschaft bleibe – aufgegriffen sowie sinngemäß durch das Zu-Wort-kommen der anwesenden Zivilgesellschaft realisiert. Dass Bildung nicht auf den schulischen Bereich zu begrenzen sei, sondern als eine Frage der Individualisierung viel umfassendere Personenkreise adressieren müsse, wurde übereinstimmend bejaht. Im Unterschied zu früher würde im Bereich des Digitalen nicht die ältere Generation die jüngere unterrichten. Tagungsgäste und Podium arbeiteten Ansätze heraus, wie den Menschen die Notwendigkeit lebenslangen Lernens deutlich gemacht werden könnte. Um die Herausforderung zu meistern, müsste beim Bedarf angesetzt werden. Speziell die Rechtswissenschaft müsste durchsichtiger und verständlicher sein, da hier der Rahmen für sämtliche Bürgerinnen und Bürger gesetzt werde. Auch wurde die Notwendigkeit vertrauensstiftender Maßnahmen angesprochen, da das Risiko des Datenmissbrauchs mittlerweile in den zahlreichen Datenbeständen selbst liegen würde. Der Kontext von Sicherheit und Freiheit wurde unter dem Stichwort informierte Einwilligung ebenfalls ausführlich diskutiert, wohingegen das bedingungslose Grundeinkommen als Kapitulation der Arbeitgeber und die in Bayern nicht vorhandene Bildungsfreistellung für Arbeitnehmer kritisiert wurden. Nichtsdestotrotz sei die deutsche Forschung von herausragender Qualität.

Bei einem feierlichen Abendprogramm auf der Veste Oberhaus, das als Abschluss den ersten Tag des Symposiums abrundete, wurde *Valerie Mocker* für ihr eminentes gesellschaftliches Engagement der For..Net Award 2019 mit der Begründung, sie verkörpere das „Geschäftsmodell Gemeinwohl“, verliehen. Europaweit gebe sie gerade den keinen kommerziellen Erfolg versprechenden innovativen Ideen zu Digitalisierung eine Chance. Diesjährige Preispatin war die Juris GmbH.

Der zweite Tag des Symposiums begann mit einem Vortrag von *Philipp Otto*, dem Direktor des Think tank iRights Lab, zum Thema „Starker Digitaler Staat – 2030 beginnt heute“ und der Frage nach der Rollendefinition Deutschlands. Er forderte unter anderem einen vom biologischen Alter losgelösten Generationenwechsel und sprach sich für einen Lösungsweg radikaler Visionen nebst einhergehendem radikalen Pragmatismus aus. Es sei notwendig, Digitalkompetenzen flächendeckend auszuweiten, beispielsweise mittels verpflichtender Masterstudiengänge für Lehramtsstudenten in „Digital Education“ sowie auch Weiterbildungsmöglichkeiten. Zudem rief *Otto* dazu auf, mit positiver Einstellung und guter Laune an die Digitalisierung heranzugehen, jeder Einzelne auf eigene Verantwortung.

Festliches Abendessen im Oberhaus (© Patrizia Fenzl)

Steve Ritter, Leiter des Rechtsreferats des Bundesamtes für Sicherheit in der Informationstechnik (BSI) fokussierte die Rol-

Gruppenfoto des Lehrstuhls in der Redoute (© Robert Geisler)

le digitaler Bildung zur Gewährleistung von IT-Sicherheit. Er verdeutlichte die Entwicklung der Digitalisierung und die Folgen der Vernetzung. Den resultierenden Vorteilen stünde auch eine Vielzahl an Risiken gegenüber, weshalb auch das Sicherheitsbewusstsein einen essentiellen Bestandteil digitaler Bildung darstelle. Durch die Vermittlung von Grundlagenkenntnissen und das Ziel, Menschen dazu anzuregen, kluge Fragen zu stellen, ließe sich bereits mit geringen Mitteln vieles erreichen. Denn es würde bei vielen bereits an der Kompetenz, IT-Systeme als sicherheitsbedürftig zu erkennen, fehlen.

Dr. Martin Scheurer widmete sich sodann der gegenwärtig signifikanten Frage möglicher Innovationsansätze, um der zunehmende datenschutzrechtlichen „Einwilligungsermüdung“ effektiv und zugleich spielerisch zu begegnen. Zur Gestaltung der Einwilligungserklärung plädierte er mit dem Konzept „form follows function“ für eine adressatengerechte Sprache, die den Einwilligenden neben der Unterrichtung vor allem bestärke, die verfügbaren Informationen auch wirklich verstehen zu können. Dies bezeichnete *Scheurer* als Frage der Opportunität. Allerdings sprach er sich gegen einen kompletten Austausch der Informationsbestandteile durch Emoticons aus, betonte aber, dass selbst gameifiziertes Datenschutzrecht insofern keine Grenzen an möglichen Einsatzgebieten setze.

Zuletzt beleuchtete *Marina Weisband*, Autorin und Leiterin des Projekts „aula – Schule gemeinsam gestalten“ von politikdigital e.V., wie aus digitaler Bildung digitale Haltung werden könne. Es gehe nicht darum, Digitalisierung in die Bildung zu integrieren, sondern in einer digitalisierten Welt Bildung zu vermitteln. Im Informationszeitalter, wo die Fachgebiete zusammenwüchsen, müsse jeder von uns sich als Pädagogin bzw. Pädagoge begreifen und aktiv an der Aus- und Fortbildung teilnehmen. Digitalisierung verleihe dem Einzelnen vermehrt Eigen- sowie Fremdverantwortung, was *Weisband* als eine Art zweite Aufklärung bezeichnete.

Unter Moderation von *Prof. Dr. Dirk Heckmann* wurde in der abschließenden Podiumsdiskussion thematisiert, wie eine Begleitung der gesamten Gesellschaft in ihrer digitalen Transformation zeitlich und finanziell konkret aussehen könnte bzw. welche Rahmenbedingungen effektiv verwirklicht werden könnten. Bisher basiere die Digitalisierung überwiegend, trotz Professionalität, auf ehrenamtlichem Engagement. Um der gegenwärtigen Existenzangst entgegenzukommen, müsste der Wert bei der kollektiven Umsetzung besser vergütet werden.

Auch im nächsten Jahr werden beim 15. Internationale For..Net-Symposium wieder interessante Impulse und interdisziplinäre Diskussionen unter dem Thema „Digitalisierung und Gemeinwohl“ geboten sein. Stattfinden wird es voraussichtlich am 23. und 24.4.2020 in Passau.

Die Aufzeichnungen der Vorträge des Symposiums können über die Webseite von For..Net (https://www.for-net.info/) abgerufen werden.

for..net
Forschungsstelle für IT-Recht und Netzpolitik

Luisa Lorenz/Julia Schwegler, Studentische Hilfskräfte am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Uni Passau.

IT-Sicherheitsgesetz 2.0: Verlässliche Sicherheit durch zertifizierte Kennzeichnung?

Zielsetzung

Innerhalb der letzten beiden Jahre ist deutschen Unternehmen durch Computerkriminalität ein Gesamtschaden in Höhe von 43,4 Milliarden Euro entstanden.[1] Nach einer Erfassung des Interessenverbandes Bitkom aus dem Jahr 2017 wurde sogar jedes zweite Unternehmen angegriffen. Eine Meldung an die Behörden erfolgt jedoch aus Angst vor Imageschäden eher selten.[2] Diese Problematik ist der Politik nicht verborgen geblieben. Um der IT-Sicherheit und dem Grundgedanken des Privacy by Design Rechnung zu tragen, sieht der Koalitionsvertrag der 19. Legislaturperiode vor, dass das Produktsicherheitsrecht novelliert und hierbei insbesondere ein europaweit gültiges IT-Sicherheits-Gütesiegel etabliert werden soll.[3] Der Käufer von mit diesem freiwilligen Kennzeichen versehenen Produkten soll in transparenter Weise über den Stand der IT-Sicherheit, insbesondere wie lange dieses mit sicherheitsrelevanten Updates seitens des Herstellers versorgt wird, informiert werden.[4]

IT-Sicherheitsgesetz 2.0 – Vorhaben und Vorteile

Dieser Maßgabe möchte der Gesetzgeber nun in der Neufassung des vier Jahre alten IT-Sicherheitsgesetzes nachkommen. Zielsetzung ist die Schaffung eines ganzheitlichen Konzepts der IT-Sicherheit für Bürger, Wirtschaft und Staat.[5] Der Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat vom 27.03.2019, zuerst veröffentlicht von netzpolitik.org[6], sieht nun in § 9a zwar kein Gütesiegel, jedoch ein freiwilliges IT-Sicherheitskennzeichen vor. Dieses Kennzeichen soll gem. § 9 Abs. 2 aus zwei Einheiten bestehen. Zum einen (Nr. 1) aus einer Erklärung des Herstellers der jeweiligen Produkte, in welcher der Hersteller das Vorliegen bestimmter IT-Sicherheitseigenschaften des Produkts für zutreffend erklärt (sog. Herstellererklärung) zum anderen einer Information des BSI[7] über Sicherheitslücken oder sonstige Informationen über sicherheitsrelevante IT-Eigenschaften (sog. BSI-Sicherheitsinformation). Diese hybride Ausgestaltung soll es dem Kunden ermöglichen, neben der Herstellererklärung über die Einhaltung einer technischen Richtlinie, eine weiterführende Information über einen Verweis (Bsp. QR-Code) zu geben, welche bei Kauf unmittelbar aufgerufen werden kann.[8]

Eine mögliche Darstellung könnte folgendermaßen aussehen: [9]

Die Verantwortung für die Herstellererklärung obliegt bei der derzeitigen Ausgestaltung rein dem Hersteller. Das BSI ist nur für die zusätzlich bereitgestellten Sicherheitsinformationen zuständig, welche jedoch eine Anreizwirkung für die Einhaltung der seitens des Herstellers getroffenen Aussagen darstellen sollen. Drohen schwerwiegende Sicherheitslü-

1 *Bitkom.* (n.d.). Schadenssummen durch Computerkriminalität in Unternehmen in Deutschland im Jahr 2018 (in Milliarden Euro). In Statista - Das Statistik-Portal. Zugriff am 23. Mai 2019, von https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/.

2 https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html Zugriff am 23. Mai 2019.

3 Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode S. 135.

4 Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode S. 44.

5 *Kipker,* MMR-Aktuell, 415455.

6 https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ Zugriff am 23. Mai 2019.

7 Bundesamt für Sicherheit in der Informationstechnik.

8 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) v. 27.03.2019 S. 63.

9 *Reisen,* IT-Sicherheitskennzeichen als Verwendungsmöglichkeit der Router-TR-Konzept BMI, 14.11.2018, S. 12, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/TR-Router-BMI.pdf?__blob=publicationFile&v=3 Zugriff am 23.05.2019.

cken, kann das BSI produktspezifisch informieren.

In der Begründung des Referentenentwurfs wird verdeutlicht, warum auf das Werkzeug eines Kennzeichens und nicht, wie im Koalitionsvertrag vorgesehen, auf ein Gütesiegel rekurriert wurde. Der klassische Ansatz eines Gütesiegels wäre nach Befürchtung des Gesetzgebers nur eine starre Momentaufnahme zum Zeitpunkt der Erteilung des Siegels.[10] IT-Sicherheit verlangt hingegen, dass sich die Validität der Kennzeichnung mit der sich wandelnden Sicherheitslage fortentwickelt. Ein zum Zeitpunkt der Zertifizierung den technischen Sicherheitsstandards entsprechendes Produkt kann innerhalb mehrerer Monate (sei es durch Sicherheitslücken in neueren Versionen oder fortentwickelte Angriffsmechanismen) potentiell bereits eine eklatante Gefahr[11] für die betriebliche oder private IT-Sicherheit darstellen. Die dynamische Ausgestaltung des Siegels ermöglicht es dem BSI hingegen nach Bekanntwerden von Sicherheitslücken eine Warnung auszusprechen, welche nicht nur ungelesen in der Nachrichtenspalte verhallt, sondern bei Aufruf des QR-Codes dem Erwerber vor Kauf präsentiert wird. Im Übrigen ermöglicht die räumliche Trennung von Produkt und zusätzlicher Information eine wesentlich bessere Information des Marktes. Auf der Produktverpackung steht nicht im hinreichenden Maß Platz zur Verfügung, um eine umfassende Aufklärung sicherzustellen. Aus diesem Grund müsste auf generische Piktogramme oder ähnliches zurückgegriffen werden. Dies ist im Hinblick auf die mannigfaltigen

Bedrohungsszenarien im Bereich der IT-Sicherheit wenig zufriedenstellend.

Nur Anschein? - eine kritische Auswertung

Bewusst spricht der Referentenentwurf nicht mehr von einem IT-Gütesiegel, sondern beschränkt sich auf die Nomenklatur des IT-Sicherheitskennzeichens. Der Aussagekraft eines Gütesiegels ist immanent, dass dieses nach einem formalisierten Prüfungsverfahren durch eine neutrale und zertifizierte Instanz auf Grund eines Gesetzes oder behördlichen Anordnung verliehen wurde.[12] Das IT-Kennzeichen beruht hingegen auf einer Selbstauskunft des Herstellers und nicht auf einer Überprüfung durch eine unabhängige Stelle. Ein auf dieser Auskunft beruhendes Gütesiegel würde den angesprochenen Verkehr in die Irre führen und genügt nicht den Erwartungen an die objektive Prüfung der für die Vergabe erforderlichen Kriterien.[13]

Neben der relativ schwachen Ausgestaltung als selbstzertifiziertes Kennzeichen sind die Freiwilligkeit der Zertifizierung und die Vergabe nur nach nationalen Vorgaben bedenklich und einer Durchsetzung möglicherweise hinderlich.

Der nationale Gesetzgeber sieht in der Gesetzesbegründung die Ausgestaltung als freiwilliges Kennzeichen als unumgänglich an. Als Begründung zieht er dabei die Vollharmonisierung des europäischen Markzugangs heran; die Einführung eines verpflichtenden Kennzeichens stelle eine Verletzung europäischen Rechts dar.[14] Richtig ist, dass nach Art. 34 AEUV mengenmäßige Einfuhrbeschränkungen sowie alle Maßnahmen gleicher Wirkung zwischen den Mitgliedsstaaten verboten sind und die Einführung einer verpflichtenden Zertifizierung für den deutschen Marktzugang zumindest eine Maßnahme gleicher Wirkung darstellen könnte. Im Bereich der IT-Sicherheit wird auf europäischer Ebene in den nächsten Monaten zudem die Verordnung über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik in Kraft treten.[15] Diese sieht in Art. 55 Abs. 1 für Hersteller oder Anbieter von zertifizierten IKT-Produkten, für welche eine EU-Konformitätserklärung ausgestellt wurde, vor, dass sie ergänzende Cybersecurityangaben, ähnlich den Vorhaben des IT-Sicherheitskennzeichens, der Öffentlichkeit zugänglich machen müssen. In Bezug auf die Freiwilligkeit ist insbesondere Art. 56 Abs. 2 und Erwägungsgrund 91 der VO von besonderem Interesse. Hiernach ist der Rückgriff auf die europäische Cybersicherheitszertifizierung und die Abgabe einer EU-Konformitätserklärung freiwillig, sofern im Unionsrecht oder im Recht der Mit-

10 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) v. 27.03.2019 S. 64.

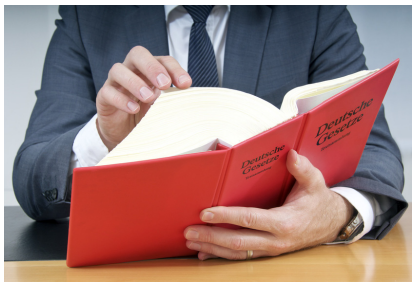
11 Im Sommer 2018 betrug die durchschnittliche Anzahl an Distributed Denial of Service (DDoS) Attacken je Angriffsziel 41. Eine veraltete Firmware oder durch Patches entstandene Schwachstellen werden durch automatisierte Angriffsprogramme auf Schwachstellen untersucht und können bereits kurz nach Kauf von diesen überwunden werden. Vgl. Akamai Technologies. (n.d.). Durchschnittliche Anzahl an DDoS-Attacken pro Angriffsziel in den Jahren 2016 bis 2018. In *Statista - Das Statistik-Portal*. Zugriff am 23. Mai 2019, von https://de.statista.com/statistik/daten/studie/756963/umfrage/durchschnittliche-anzahl-an-ddos-attacken-pro-ziel-je-quartal/.

12 *Pfeifer/Obergfell* in Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG, 3. Aufl. 2016, Band 2 § 5 Rn. 306d.

13 *OLG Köln*, Beschluss v. 05.03.2018 – 6 U 151/17 – GRUR-RS 2018, 4892.

14 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) v. 27.03.2019 S. 64.

15 PE-CONS 86/1/18 Rev 1.



gliedsstaaten nichts Anderes festgelegt ist. Der Erlass technischer Vorschriften richtet sich insbesondere nach der Richtlinie (EU) 2015/1535. Diese Richtlinie umfasst insbesondere nach Art. 1 Abs. 1 lit. a) Regelungen für Erzeugnisse, die gewerblich hergestellt werden und versteht unter technischen Vorschriften gem. Art. 1 Abs. 1 lit. f „technische Spezifikationen oder sonstige Vorschriften […] deren Beachtung rechtlich oder de facto für das Inverkehrbringen […] verbindlich ist […]". Ein nationales verbindliches IT-Sicherheitskennzeichen könnte als eine derartige technische Spezifikation angesehen werden, nach welcher Produkte nur nach erfolgter Zertifizierung in Deutschland in den Verkehr gebracht werden dürften. Die Richtlinie verbietet die Einführung solcher nationalen Regelungen demnach nicht absolut, sondern knüpft diese unter anderem an die Notwendigkeit der vorhergehenden Information der Kommission und die Darlegung der Gründe, die die Festlegung einer derartigen technischen Vorschrift erforderlich machen, Art. 5 RL (EU) 2015/1535. Diese, zugegebenermaßen sehr formale, Darstellung besagt in ihrem Kern, dass der europäische Gesetzgeber eine Zertifizierung grundsätzlich auf freiwilliger Basis ansieht, den Mitgliedsstaaten jedoch die Option offenlässt, auf nationaler Ebene durchaus verpflichtende Regelungen zu treffen.

Der zukünftige Cybersecurity Act verdeutlicht auch, dass die Erarbeitung einer Zertifizierung sinnvollerweise nicht unabhängig durch die einzelnen Mitgliedsstaaten erfolgen sollte. Wie auch seitens des Interessenverbandes Bitkom gefordert[16], sind unter Praktikabilitätsgesichtspunkten die Anforderungen an ein Sicherheitskennzeichen in Zukunft durch supranationale Normungsorganisationen zu erarbeiten. Dies auch unter dem Gesichtspunkt, im europäischen Wirtschaftsraum einen unangebrachten und oftmals intransparenten Wettbewerb unterschiedlicher nationaler Zertifikate zu unterbinden.

Im Hinblick auf den Verbraucherschutz ist die Einführung einer sichtbaren Zertifizierung grundsätzlich ein zu begrüßendes Unterfangen. Die Sensibilisierung des Verbrauchers und die Aktualität der seitens des BSI bereitgestellten Informationen zählen zu den größten Vorteilen, die das Vorhaben verspricht. Schade ist, dass die Chance zur Vergabe eines abgestuften Kennzeichens nicht wahrgenommen wurde. Auf den ersten Blick und ohne Abruf des QR-Codes kann der Käufer lediglich erkennen, dass ein Produkt zum Zeitpunkt der Vergabe zumindest den Mindestanforderungen der IT-Sicherheit genügt. Ob das gekennzeichnete Produkt jedoch tatsächlich sicherer ist als das der Mitbewerber oder wie hoch der tatsächliche Schutz ist, bleibt verborgen. Im Übrigen verbleibt weiterhin eine große Verantwortung auf Seiten des Käufers. Der Hersteller mag für den angegebenen Zeitraum ausreichend Sicherheitsupdates bereitstellen, sofern der Käufer diese nicht installiert erhöht sich die IT-Sicherheit des Gerätes effektiv nicht. Es besteht die Gefahr, dass der Käufer sich auf das Kennzeichen verlässt und sich in vollkommener Sicherheit wägt. Gerade im digitalen Kontext und der Mannigfaltigkeit der Bedrohungsszenarien sollten Verwender zu jedem Zeitpunkt einen sorgsamen Umgang bedenken.

Als problematisch ist ferner hervorzuheben, dass eine Selbstzertifizierung immer die Gefahr von Manipulationen und Ungenauigkeiten mit sich bringt. Verstärkt wird dies dadurch, dass die Neuregelung für das BSI ausdrücklich keine Pflicht, sondern nur die reine Möglichkeit der Überprüfung der Angaben vorsieht. Sollte sich das Kennzeichen marktweit durchsetzen und keine nennenswerte Aufstockung der personalen Kapazitäten des BSI stattfinden, ist damit zu rechnen, dass mit steigender Anzahl der Zertifizierungen die Dunkelziffer der falschen Herstellerangaben zunehmen dürfte. Dies auch deswegen, da eine eventuelle Falschangabe des Herstellers nicht gem. § 14 des IT-SiG 2.0 als Ordnungswidrigkeit qualifiziert wird und daher nicht durch das scharfe Schwert des Bußgeldes finanziell sanktioniert werden kann.

Fazit und Auswirkungen auf die Praxis

Das IT-Sicherheitskennzeichen ist ein erster zaghafter Versuch, das IT-Sicherheitsverständnis in der Präsenz der breiteren Masse zu verankern und in dieser Thematik zu sensibilisieren. Sollte sich diese Praxis im Markt etablieren können, stellt das Führen einen nicht zu unterschätzenden Marktvorteil dar. Abzuwarten bleibt, ob das deutsche Kennzeichen auch auf dem europäischen und internationalen Markt Anerkennung finden wird oder ob in absehbarer Zeit eine Ersetzung durch ein allgemeines europäisches Kennzeichen erfolgen wird. Für eine wirksame Sensibilisierung des Marktes ist erforderlich, dass die Erwerber sich auf ein verlässliches und aussagekräftiges Kennzeichen verlassen können. Sollte es zu einer Flut unterschiedlicher Kennzeichen wie im Bio-Siegel-Sektor kommen, deren Kenntnis bzw. Vertrauen bei den Verbrauchern sehr beschränkt ist[17], wäre die erwünschte Wirkung nicht gegeben.

Neben Auswirkungen für Hersteller technischer Geräte bietet das Kennzeichen auch Chancen und Risiken für alle kleinen und mittelständischen Unternehmen. Sollten betriebsintern keine dezidierten IT-Kenntnisse vorhanden sein, kann das Vorliegen (oder Fehlen) eines IT-Sicherheitskennzeichens einen laienverständlichen Hinweis auf mögliche Gefährdungspotentiale darstellen. Dabei sollte jedoch kein blindes Vertrauen in die Richtigkeit und Aktualität der Informationen gesetzt werden, sondern jedes Kennzeichen vor Kauf und über den kompletten Zeitraum des Einsatzes regelmäßig erneut abgerufen werden. Es ist ratsam, im Rahmen der betrieblichen Organisation einen regelmäßigen Abruf- und Überprüfungsplan aufzustellen.

Ass. jur. Lukas Schmidt

16 *Bitkom*, Stellungnahme zum IT-Sicherheitskennzeichen v. 09.04.2019 S. 3.

17 *Statista.* (n.d.). Wie gut kennen bzw. wie sehr vertrauen Sie folgenden Bio-Siegeln?. In Statista - Das Statistik-Portal. Zugriff am 31. Mai 2019, von https://de.statista.com/statistik/daten/studie/705842/umfrage/umfrage-zur-kenntnis-von-bio-siegeln-in-deutschland/.

WhatsApp-Nutzung im Unternehmen

WhatsApp[1] und ähnliche Messenger Dienste[2] sind ein mittlerweile fest etabliertes Medium in der deutschen Kommunikationswelt und werden von vielen im Rahmen der täglichen Kommunikation genutzt.[3] Diese Messengerdienste haben die Nutzung von SMS weitgehend abgelöst. Selbst Dateien können mit Hilfe vieler der internetgestützten Messenger schnell und einfach verschickt werden. Aus diesem Grund erfährt die Nutzung von Messenger-Apps auch im Berufsleben eine Zunahme. Datenschutzrechtlich wird z.B. die Nutzung von WhatsApp durchaus als kritisch gesehen.[4] Ob und welche Risiken hier hinsichtlich Daten- und IT-Sicherheit bestehen und welche Folgen dies für die Nutzung (bzw. arbeitgeberseitigen Erlaubnis der Nutzung) hat, soll im Folgenden dargestellt werden. Hierbei soll WhatsApp als in Deutschland wohl bekannteste Telekommunikations-App stellvertretend für eine Reihe ähnlich funktionierender Applikationen stehen. WhatsApp nutzt hierbei eine zusätzliche Methode, mit der sich die Endgeräte der Kommunikationspartner gegenseitig überprüfen können und feststellen, ob dazwischengeschaltete Dritte die Kommunikationsdaten abgreifen.[5]

IT-sicherheitsrelevante Funktionsweise von WhatsApp

Der Kommunikationsdienst WhatsApp nutzt eine Ende-zu-Ende-Verschlüsselung.[6] Hierbei werden die Kommunikationsdaten grundsätzlich so verschlüsselt, dass Dritte diese nicht einsehen können; nach Angaben von WhatsApp auch nicht der Anbieter selbst.[7] Bei der Ende-zu-Ende-Verschlüsselung (im Englischen „end-to-end encryption“[8]) findet die Ver- und Entschlüsselung jeweils an den Endpunkten der Übertragung statt.[9] Die Entschlüsselungs-Schlüssel sind nur auf den jeweiligen Endgeräten gespeichert.[10] Damit beide Geräte auf die Kommunikationsdaten zugreifen können, müssen diese zuvor den Schlüssel vereinbart und ausgetauscht haben.[11] Hier wird zunächst ein öffentlicher und jedermann zugänglicher Schlüssel verwendet (Public-Key). Mit einem solchen Schlüssel verschlüsselte Daten lassen sich wiederum nur mit dem dazugehörigen privaten Schlüssel (Private-Key) entschlüsseln. Vor der eigentlichen Kommunikation findet daher kein Austausch der privaten Schlüssel statt.[12]

IT-Sicherheitsvorfälle

Zunächst ist festzustellen, dass WhatsApp ebenso wie sämtliche, zumindest aber der Großteil IT-gestützter Systeme dem ständigen Risiko von Hacker-Angriffen ausgesetzt ist. So sind z.B. im vergangen Monat Lücken in der IT-Sicherheitsstruktur von WhatsApp bekannt geworden, die einen Zugriff von Hackern auf die Mobiltelefone der App-Nutzer ermöglichte.[13] Der Angriff erfolgte über einen Sprachanruf an die betroffenen Nutzer, über welchen die entsprechende Schad- und Spionagesoftware auf den jeweiligen Mobiltelefonen installiert wurde – dies nach Vermutungen sogar ohne, dass das Annehmen des Anrufs nötig war. Methodisch handelte es sich um einen sog. „buffer overflow“, bei welchem auf den von WhatsApp vorgesehenen Speicherbereich zu große Datenmengen geschrieben werden und hierdurch letztlich das Überschreiben anderer Speicherbereiche möglich wird.[14] Das gefährliche hieran war, dass das Hacken der end-

1 WhatsApp ist eine Nachrichtenaustausch Applikation die eine Variation von Funktionen zulässt. Hierzu zählen das Versenden von Text- und Bildnachrichten, die Internettelefonie mit Bildübertragungen, das Versenden von Sprachaufnahmen, etc. vgl. Whatsapp, https://www.whatsapp.com/features/, zuletzt abgerufen am 24.05.2019.

2 Z.B. Telegram, Facebook Messenger, Snapchat, Line, etc.

3 56 % der Deutschen YouGov Studie von Greven Medien, *Greven*, https://www.greven.de/messenger-marketing-umfrage, zuletzt abgerufen am 24.05.2019.

4 *Jung/Hansch,* Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen, ZD 2019, 143, 145.

5 *Scherschel,* heise security, https://m.heise.de/security/artikel/Test-Hinter-den-Kulissen-der-WhatsApp-Verschluesselung-3165567.html, zuletzt abgerufen am 29.05.2019.

6 *WhatsApp,* FAQ, https://faq.whatsapp.com/de/android/28030015/, zuletzt abgerufen am 20.05.2019, viele weitere Dienste nutzen ebenfalls diese Verschlüsselungsmethode, vgl. iMessage, https://support.apple.com/de-de/HT209110, Telegram, https://telegram.org/faq/de#geheime-chats, sämtliche zuletzt abgerufen am 29.05.2019.

7 *WhatsApp,* FAQ, https://faq.whatsapp.com/de/android/28030015/, zuletzt abgerufen am 20.05.2019.

8 *Witte,* heise online, https://www.heise.de/tipps-tricks/Ende-zu-Ende-Verschluesselung-was-genau-ist-das-4007116.html, zuletzt abgerufen am 29.05.2019.

9 *Witte,* heise online, https://www.heise.de/tipps-tricks/Ende-zu-Ende-Verschluesselung-was-genau-ist-das-4007116.html, zuletzt abgerufen am 29.05.2019.

10 *SearchSecurity,* https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EEm zuletzt abgerufen am 29.05.2019.

11 *Luber/Schmitz,* Security Insider, https://www.security-insider.de/was-ist-ende-zu-ende-verschluesselung-e2ee-a-727147/, zuletzt abgerufen am 29.05.2019.

12 *Luber/Schmitz,* Security Insider, https://www.security-insider.de/was-ist-ende-zu-ende-verschluesselung-e2ee-a-727147/, zuletzt abgerufen am 29.05.2019.

13 *O'Sullivan,* CNNBusiness, https://edition.cnn.com/2019/05/14/tech/whatsapp-attack/index.html, zuletzt abgerufen am 24.05.2019.

14 *Thomson,* The Register, https://www.theregister.co.uk/2019/05/14/whatsapp_zero_day/, zuletzt abgerufen am 05.06.2019.

to-end Verschlüsselung der WhatsApp Kommunikation nicht mehr erforderlich wird, weil der WhatsApp Code selbst bereits überschrieben werden kann.[15]

Eine weitere Schwachstelle, die Sicherheitsforscher von Check Point entdeckt hatten, ermöglichte es Angreifern eingangs vertrauensvolle Nachrichten abzufangen, zu manipulieren und anschließend falsche Nachrichten im Namen unbeteiligter Nutzer zu versenden.[16] Nach Aussage der Sicherheitsforscher schaffte dieser Sicherheitsmangel die Möglichkeit, umfangreich Falschinformationen zu schaffen und zu verbreiten, mit dem Anschein, dass diese von vertrauenswürdigen Quellen stammen. Anders gesprochen bedeutet dies, dass es möglich ist, beliebigen Personen Wörter in den Mund zu legen.

Entgegen einer nachvollziehbaren ersten Reaktion auf diese Nachrichten, kann trotz der beschriebenen Sicherheitsvorfälle nicht davon ausgegangen werden, dass WhatsApp ein außergewöhnlich hohes Sicherheitsrisiko darstellt. IT-Sicherheitsvorfälle in Form von versteckten Virenprogrammen sind gerade bei herkömmlichen Kommunikationsmethoden wie z.B. E-Mail nichts Unbekanntes. Auch das Bundesamt für Sicherheit in der Informationstechnik warnt nicht vor der Nutzung von Instant Messengern, rät allerdings zu gewissen Vorsichtsmaßnahmen.[17]

Grundlegendes zum Datenschutz im Unternehmen

Der Datenschutz hat in Unternehmen an vielerlei Schnittstellen eine Berücksichtigung zu finden und hat hierbei jeweils eine besondere IT-sicherheitsbezogene Komponente. Dies zeigt sich etwa daran, dass der Verantwortliche für die Verarbeitung personenbezogener Daten gem. Art. 32 DS-GVO unter Androhung von Bußgeldern bis zu 20.000.000,00 Euro (Art. 83 Abs. 5 DS-GVO)[18] nach den Vorgaben der DS-GVO dazu zwingend angehalten ist, technische und organisatorische Maßnahmen (sog. TOMs) vorzuhalten, um die Datensicherheit zu gewährleisten. Mit Hinblick auf die IT-Sicherheit eines Unternehmens und den Vorgaben der DS-GVO besonders zu beachten, sind etwa Fragen des BYOD (Bring your own device). Ist es Arbeitnehmern etwa gestattet, eigene IT-Geräte, also auch Mobiltelefone zur Erledigung dienstbezogener Aufgaben zu nutzen, ist naheliegend, dass Arbeitnehmer gängige Messenger Systeme wie etwa WhatsApp nutzen. Durch die Nutzung von Kommunikationsdiensten auf einem privaten Mobiltelefon ändert sich an der Zuordnung des Arbeitgebers als datenschutzrechtlich Verantwortlichem grundsätzlich nichts (vorausgesetzt der Arbeitnehmer handelt im Rahmen seiner arbeitsvertraglichen Pflichten).[19]

Mitarbeiterdaten / Beschäftigtendatenschutz

Die Vorschriften der DS-GVO gelten auch für den Beschäftigtendatenschutz, also unter anderem im Verhältnis Arbeitgeber zu Arbeitnehmer. Gem. Art. 88 DS-GVO kann der Beschäftigtendatenschutz durch die Mitgliedsstaaten konkretisiert werden. Mit Art. 26 BDSG ist der nationale Gesetzgeber dem nachgekommen. Da es hierbei vorrangig um die Rechtfertigung einer Datenverarbeitung geht, soll hierauf zunächst nicht weiter eingegangen werden. Allerdings ist auch im Bereich des Beschäftigtendatenschutzes festzuhalten, dass die besonderen Voraussetzungen einer rechtmäßigen Datenverarbeitung eingehalten werden müssen. Hierzu gehört das Vorhalten technischer und organisatorischer Maßnahmen, um unter anderem ein ungewolltes Nachaußengelangen der Daten zu verhindern.

Kundendaten

WhatsApp lässt sich nicht nur für die unternehmensinterne Kommunikation nutzbar machen, sondern auch innerhalb der Kundenbeziehung. Hierbei können z.B. Arztpraxen Termine nicht via Telefon sondern über den Messenger Service WhatsApp ausmachen.[20] Einige Apotheken etwa haben den Kommunikationsdienst auch schon als Medium zur Bestellung von rezeptpflichtigen Medikamenten eingesetzt. Hierbei konnten Kunden ihre Rezepte per Foto über WhatsApp an die Apotheke versenden.[21] Als datenschutzrechtlich kritisch wird etwa vom Bundesbeauftragten für den Datenschutz und die Informationssicherheit bemängelt, dass in Verbindung von WhatsApp und Facebook Kontaktdaten, die auf den Mobiltelefonen der WhatsApp Nutzer gespeichert sind, automatisch hochgeladen werden.[22] Der Datenschutzbeauftragte hatte daher bereits im Mai 2017 diese Praxis beanstandet, befindet sich aber derzeit noch in der weiteren Erörterungsphase mit Verantwortlichen des Unternehmens. Auch die Landesbeauftragte für den Datenschutz Niedersachsen hat die betriebliche Kommunikation in Unternehmen via WhatsApp als Verstoß gegen die DS-GVO beanstandet.[23] Das WhatsApp einsetzende Unternehmen ist für die Übersendung der Kontaktdaten verantwortlich im Sinne der DS-GVO, die Verantwortung ist also nicht an WhatsApp abgeschoben. Eine nach Art. 6 Abs. 1 DS-GVO erforderliche Rechtsgrundlage für die Übermittlung wird schwer zu finden sein. Eine entsprechende Nutzung von WhatsApp muss daher sorgfältig überlegt sein. Werden

15 *Thomson*, The Register, https://www.theregister.co.uk/2019/05/14/whatsapp_zero_day/, zuletzt abgerufen am 05.06.2019.

16 *Barda/Zaikin/Vanunu*, Check Point, FakeApp: A Vulnerability in WhatsApp, https://research.checkpoint.com/fakesapp-a-vulnerability-in-whatsapp/, zuletzt abgerufen am 24.05.2019.

17 *BSI*, Instant Messenger: Tipps, https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/Messenger/Tipps/tipps_node.html, zuletzt abgerufen am 05.06.2019.

18 Ggf. sogar höher, wenn etwa 4% des gesamten weltweit erzielten Jahresumsatzes des Unternehmens diese Summe überschreiten sollte, vgl. § 84 Abs. 5 Alt. 2 DS-GVO.

19 *Helfrich*, in: Forgó/Helfricht/Schneider, Betrieblicher Datenschutz, 2019, Kapitel 2, Rn. 31 ff.

20 Vgl. Hinweis hierauf vom *Bayerischen Landesamt für Datenschutz*, 7. Tätigkeitsbericht 2015/2016, https://www.lda.bayern.de/media/baylda_report_07.pdf, Seite 138, zuletzt abgerufen am 29.05.2019.

21 *Thiel*, Landesbeauftragte für den Datenschutz Niedersachsen, DuD 2018, 601.

22 *Bundesbeauftragte für den Datenschutz und die Informationssicherheit*, Anlage zur Pressemitteilung für den 27. Tätigkeitsbericht zum Datenschutz – Ausgewählte Themen, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/AnlagePM_27TB.html?nn=5217154, beides zuletzt abgerufen am 29.05.2019.

23 *Thiel*, Landesbeauftragte für den Datenschutz Niedersachsen, DuD 2018, 601.

dann auch noch Microsoft Outlook und WhatsApp gleichzeitig auf dem Mobiltelefon genutzt, so sollten wenigstens technische Vorkehrungen getroffen werden, um einen Zugriff von WhatsApp auf (zumindest) Kundendaten zu unterbinden.[24] Betroffen sind hier zwar keine sensiblen Daten oder besondere kundenspezifische Kommunikationsinhalte, die Weitergabe von Kunden-Kontaktdaten an Facebook erfolgt ansonsten aber ohne weitere Kontrolle. Die Übermittlung der Kontaktdaten kann darüber hinaus als Verstoß gegen das Prinzip der Datensparsamkeit (Art. 5 Abs. 1 c) DS-GVO) gesehen werden und damit nicht zuletzt ein Verstoß des Verantwortlichen gegen die Pflicht mittels geeigneter technischer und organisatorischer Maßnahmen die Datenschutzgrundsätze wirksam einzuhalten.[25]

WhatsApp-Nutzung im Unternehmen untersagen

Wird die WhatsApp Nutzung innerhalb des Betriebs oder zu betrieblichen Zwecken als zu unsicher empfunden, so ist es dem Arbeitgeber als Teil seines Weisungsrechts überlassen, die Nutzung zu untersagen. Schwieriger ist dies, wenn die Nutzung des privaten Mobiltelefons zu betrieblichen Zwecken gestattet wird. Hier sollte zumindest eine technische Trennung von betrieblicher Nutzung und privater Nutzung eingerichtet werden, um die Kontaktdatenübermittlung via WhatsApp zu unterbinden.

Die Untersagung von WhatsApp aus IT-Sicherheitsperspektive kann sich für einen Arbeitgeber unter anderem aus Gründen des betrieblichen Geheimnisschutzes als notwendig darstellen. Die Geheimhaltungspflichten des Arbeitnehmers sind bereits arbeitsvertragliche Nebenpflicht, § 241 Abs. 2 BGB.[26] Das im April 2019 in Kraft tretende Geschäftsgeheimnisgesetz (GeschGehG) hat die Aufmerksamkeit auf das Erfordernis eines angemessenen Informationsschutzes in Unternehmen noch einmal verstärkt.[27] Der Informationsschutz ist also sowohl aus Geschäftsgeheimnisgründen, Datenschutzgründen als auch unter Berücksichtigung des IT-Sicherheitsrechts zu beachten. Insofern WhatsApp für die Erfordernisse des Unternehmens also keine hinreichende Sicherheit bieten kann (u.a. auch aufgrund fehlender Kontrollmöglichkeiten[28]), ist die grundsätzliche Untersagung einer betrieblichen Nutzung von WhatsApp und ähnlich funktionierenden Messengern bzw. die Nutzung dieser Dienste auf dienstlichen Handys nur eine angemessene Wahrnehmung arbeitgeberseitigen Interesses.

Darüber hinaus sind Fälle denkbar, bei denen aufgrund des besonders sensibles Berufsfeldes, die Nutzung von WhatsApp zu strafrechtlichen Konsequenzen wegen Verletzung des Privatgeheimnisses gem. § 203 StGB führen könnte. Hier bedarf es daher besonderer Vorsicht.

Fazit

Eindeutig bewerten lässt sich die arbeitgeberseitige Gestattung von WhatsApp oder ähnlichen Messengern im Unternehmen nur schwer. Lange gab es hierzu auch keine datenschutzrechtliche Festlegung seitens der Aufsichtsbehörden.[29] Aufgrund der Ende-zu-Ende Verschlüsselung ist zumindest aus IT-sicherheitstechnischer Perspektive ein relativ hohes technisches Schutzniveau gegeben. Das Abfangen und Lesen von Kommunikationsinhalten ist daher mit zumindest höherem Aufwand verbunden. Es lässt sich auch nicht eindeutig sagen, dass alternative Kommunikationsmöglichkeiten innerhalb eines Unternehmens eine höhere Sicherheit und damit die datenschutzrechtlich und IT-technisch geeignetere Alternative darstellen. Zumindest bei der Verarbeitung besonders sensibler Daten (vgl. Art. 9 DS-GVO) sollte jedoch auf eine besondere Verschlüsselung der Informationsdaten geachtet werden. Soweit eine IT-sicherheitsrechtliche Betrachtung die Verwendung von WhatsApp in Unternehmen also zulässt, stellen sich datenschutzrechtlich weitläufigere Probleme. Aus datenschutzrechtlicher Perspektive darf bereits jetzt die automatische Verknüpfung der auf dem Mobiltelefon gespeicherten Kontaktdaten mit WhatsApp als unzulässig beurteilt werden. Hier sollte der Aufwand betrieben werden, anhand technischer Maßnahmen die Verknüpfung mit Kundendaten zu verhindern. Damit einhergehende Funktionseinschränkungen sind dann in Kauf zu nehmen.

Jannik Zerbst, LL.M. (VUW)

24 *Faas,* ArbRAktuell 2018, 594.

25 So *Thiel,* Landesbeauftragte für den Datenschutz Niedersachsen, DuD 2018, 601, 602.

26 *Schubert,* Kommentar zum europäischen Arbeitsrecht, 2018, RL 2016/943/EU Art. 2, Rn. 4ff.

27 *Voigt/Herrmann/Grabenschröer,* BB 2019, 142, 144.

28 Siehe zur arbeitsrechtlichen Problematik der Vermengung von privater und dienstlicher Kommunikation über das gleiche Kommunikationsmedium am Beispiel von E-Mail Kommunikation vgl. *Brink/Schwab,* ArbRAktuell 2018, 111.

29 *Bayerisches Landesamt für Datenschutz,* 7. Tätigkeitsbericht 2015/2016, https://www.lda.bayern.de/media/baylda_report_07.pdf, Seite 138, zuletzt abgerufen am 29.05.2019.

Malvertising – Gefahr durch Online-Werbung

Jeder Internetnutzer trifft beim Surfen durch das Web nahezu täglich auf sie: Die Online-Werbung. Aus unternehmerischer Sicht stellt Online-Werbung eine wirtschaftlich lukrative Möglichkeit dar, Produkte und Dienstleistungen einer Vielzahl von Menschen anbieten zu können, ohne mit diesen persönlich in Kontakt treten zu müssen. Diese Form der Werbung ist im Grundsatz ein legitimes Mittel für Werbetreibende, jedoch treten dann Probleme auf, wenn dadurch die „User Experience“[1] beeinträchtigt wird. Dabei ist zu beachten, dass nicht nur Privatpersonen betroffen sein können, sondern diese Gefahr auch für Unternehmen besteht, wenn Arbeitnehmer beispielsweise die Firmenrechner zum privaten Surfen gebrauchen dürfen.[2]

Die Aktualität dieses Themas offenbart sich unter anderem dadurch, dass diese Woche bekannt geworden ist, dass Nutzer, die Windows 10 Apps aus dem Microsoft Store nutzen, mit schädlicher Werbung – dem sogenannten Malvertising – rechnen müssen.[3]

Was ist Malvertising

Malvertising ist ein aus dem Englischen stammender Begriff und setzt sich aus den Wörtern Malware (dt.: „Schadcode“) und Advertising (dt.: „Werbung“) zusammen. Beim Malvertising wird Schadsoftware über manipulierte, aber häufig auch über legal eingekaufte Online-Werbeeinblendungen auf die Endgeräte der Nutzer gespielt. Indem kriminelle Werbeplätze bei Werbenetzwerken oder direkt beim jeweiligen Unternehmen anmieten, können diese die schädliche Werbung, meist sehr günstig, an eine Vielzahl von Personen richten.[4] Neben der Infizierung mit Schadprogrammen umfasst der Begriff des Malvertisings aber auch andere Vorgänge, wie das Setzen von Tracking-Cookies oder die vom Nutzer nicht autorisierte Installation von an sich rechtmäßiger Software. Diese werden in der Folge dazu missbraucht, vom Nutzer unerkannt, persönliche Informationen oder verhaltensspezifische Informationen über die Internetnutzung abzugreifen.[5]

Welche Arten von Malvertising gibt es und wie funktionieren sie?

Malvertsing tritt grundsätzlich in zwei verschiedenen Arten auf. Die unmittelbare Infektion des Gerätes mit der schädlichen Werbung oder die mittelbare Infektion des Gerätes, die zusätzlich einer Handlung des Nutzers bedarf. Die unmittelbare Infektion wird in Form von Drive-By-Infektionen durchgeführt, die direkt in die aufgerufene Webseite, beispielsweise als Pop-Up, iFrame, Flash-Erweiterung oder in das Java-Skript, eingebunden werden. Hierbei werden durch die Erstellung eines entsprechenden Codes (sog. „Exploit“[6]) Sicherheitslücken im Browser oder deren Plugins ausgenutzt.[7]

Die mittelbare Infektion eines Geräts erfolgt dadurch, dass der Nutzer selbst aktiv auf die ihm angezeigte Online-Werbung klickt. Diese leitet den Nutzer im Anschluss auf eine manipulierte Webseite oder es öffnet sich ein Pop-Up Fenster auf dem die Exploits zur Anwendung kommen.[8] Diese Art der Infektion findet derzeit bei den Windows 10 Apps statt. Hier geben Webseiten vor, dass der Nutzer einen Preis gewonnen habe oder dass sein PC von Schadsoftware befallen sei, weswegen er ein vermeintliches Anti-Virenprogramm herunterladen müsse. Durch diese Meldungen soll der Nutzer zur Interaktion aufgerufen werden, um den entsprechenden Exploits den Weg auf sein Gerät zu ermöglichen.[9]

Schutz vor Infektion durch Malvertising

Zwar ist die Infektion durch Malvertising akut, jedoch gibt es eine Reihe von Möglichkeiten, die Unternehmen ergreifen

1 https://it-service.network/blog/2018/11/09/malvertising/ (Zuletzt abgerufen am 07.06.19).

2 https://it-service.network/blog/2018/11/09/malvertising/ (Zuletzt abgerufen am 07.06.19).

3 https://answers.microsoft.com/de-de/windows/forum/all/windows-apps-%C3%B6ffnen-fake-webseiten-mit/62d2039d-8c3a-4684-a994-d43cff7bd7ab?auth=1 (Zuletzt abgerufen am 07.06.19).

4 Vgl. https://it-wegweiser.de/malvertising/ (Zuletzt abgerufen am 07.06.19).

5 Vgl. https://www.kaspersky.de/blog/was-ist-malvertising/3917/ (Zuletzt abgerufen am 07.06.19).

6 https://it-wegweiser.de/malvertising/ (Zuletzt abgerufen am 07.06.19).

7 https://it-wegweiser.de/malvertising/ (Zuletzt abgerufen am 07.06.19).

8 https://it-wegweiser.de/malvertising/ (Zuletzt abgerufen am 07.06.19).

9 https://www.heise.de/security/meldung/Malvertising-Microsoft-warnt-vor-verseuchten-Werbeanzeigen-in-Windows-10-Apps-4437094.html (Zuletzt abgerufen am 07.06.19).

können, um sich vor schädlicher Werbung zu schützen.

Den Nutzern, der oben angesprochenen Windows Apps ist besonders zu empfehlen, die vom Malvertising betroffenen Domains - *.adnxs.com*, *.nuxues.com* und *.vungle.com* - zu meiden. Da derzeit allerdings noch nicht bekannt ist, in welchen Apps Werbung über diese Domains eingespielt wird, erscheint es derzeit sinnvoll, diese Domains durch einen Adblocker im Browser komplett zu blockieren.[10]

Eine weitere allgemeine und effektive Methode für Unternehmen ist, ihre Mitarbeiter präventiv auf die Gefahren, die durch Malvertising entstehen können, hinzuweisen und im Umgang mit unbekannten Webseiten zu schulen. Ratsam ist zudem, ausschließlich Webseiten aufzurufen, die eine sichere Datenübertragung gewährleisten. Ob es sich bei der angewählten Webseite um eine „sichere" Webseite handelt, kann der Nutzer selbst prüfen, indem er nachsieht, ob für die Webseite ein Verschlüsselungszertifikat (SSL/TLS) besteht.[11] Zudem sollten Webseiten gemieden werden, die den Nutzer zum Log-in auf eine andere Webseite leiten. Diese zweite Webseite ist oftmals mit Schadsoftware infiziert oder dient Phishing-Attacken.[12] Ein weiteres nützliches Mittel zur Abwehr von Malvertising ist das fortlaufende updaten des Betriebssystems, des Browers und der Plugins, da dortige Sicherheitslücken das Malvertising gerade erst ermöglichen. Die wohl effektivste Maßnahme zur Vermeidung

einer Infektion durch Malvertising ist ein umfassender Einsatz von Adblockern. Diese verhindern bereits, dass die schädliche Werbung beim Nutzer angezeigt wird.[13]

Fazit

Aufgrund der täglichen Nutzung des Internets in Unternehmen und des Umstands, dass jederzeit eine Malvertising-Attacke droht, sind Schutzmaßnahmen hiergegen notwendig. Bereits durch die Umsetzung der oben genannten Maßnahmen kann die Wahrscheinlichkeit einer Infizierung durch Malvertising um ein Vielfaches reduziert werden. Dies erscheint auch aus wirtschaftlichen Gesichtspunkten äußerst sinnvoll, da die Kosten für präventive Sicherheitsmaßnahmen meist weitaus geringer ausfallen, als für repressive Maßnahmen zur Behebung der Folgen des Malvertisings. Zudem dienen diese Maßnahmen als Teilaspekte einer umfassenden IT-Sicherheitsstrategie eines Unternehmens nicht nur der Abwehr einer Infizierung durch schädliche Werbung, sondern auch anderer Schadsoftware. Diese Hinweise sollten jedoch nicht dahingehend verstanden werden, dass Online-Werbung grundsätzlich schädliche Wirkung für die IT-Systeme im eigenen Unternehmen hat. So ist der überwiegende Teil von Online-Werbung freilich nicht von schädlicher Natur, sondern kann den Nutzer durchaus auf nützliche Produkte oder Dienstleistungen hinweisen. Insoweit kommt es gerade auf eine ausgeglichene Balance zwischen der Ergreifung von Sicherheitsmaßnahmen zum Schutz der eigenen IT-Systeme und einer sinnvollen Informationsgewinnung durch Online-Werbung an.

Jurist (Univ.) Lukas Fleischer

10 https://www.heise.de/security/meldung/Malvertising-Microsoft-warnt-vor-verseuchten-Werbeanzeigen-in-Windows-10-Apps-4437094.html (Zuletzt abgerufen am 07.06.19).

11 https://it-service.network/blog/2018/10/04/ssl-zertifikat/ (Zuletzt abgerufen am 07.06.19).

12 https://it-service.network/blog/2018/11/09/malvertising/ (Zuletzt abgerufen am 07.06.19).

13 https://www.heise.de/security/meldung/Malvertising-Microsoft-warnt-vor-verseuchten-Werbeanzeigen-in-Windows-10-Apps-4437094.html (Zuletzt abgerufen am 07.06.19).

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.

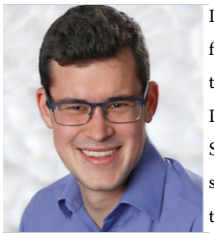
Jannik Zerbst, LL.M. (VUW)

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.

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.

Lukas Fleischer



Lukas Fleischer hat Anfang 2019 sein Erstes Juristisches Staatsexamen in Passau abgeschlossen. Seither arbeitet er als wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau. Ebenfalls seit Beginn dieses Jahres befindet sich Lukas Fleischer im juristischem Vorbereitungsdienst.

Das nächste Magazin erscheint am 15. September 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.