Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 B

Stellungnahme zum Antrag "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken"

Prof. Dr. rer. nat. Rüdiger Weis, Diplom-Mathematiker, Berlin

Stellungnahme zum Antrag "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken" des Ausschusses für Inneres und Heimat des Deutschen Bundestages im Rahmen der Öffentlichen Anhörung des Ausschusses für Inneres und Heimat am Montag, dem 27. Januar 2020 zum Antrag der Fraktion der FDP "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken" - BT-Drucksache 19/5764

- Prof. Dr. rer. nat. Rüdiger Weis, Diplom-Mathematiker, Berlin
- Zusammenfassung Stellungnahme: "Recht auf Verschlüsselung"

Bei der Analyse der Sicherheit von Computernetzwerken geht man in der theoretischen Modellbildung von sehr mächtigen Angreifern aus, die alle Nachrichten mitlesen und verändern kann. Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingesetzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder nahezu für jeden Motivierten brechbar ist. Diese Eigenschaft verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten. Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergerführt, erweitert und intelligent verstetigt werden.

Sicherheitslücken können mit Hilfe von Angriffswerkzeugen ausgenutzt werden, bei denen es sich um kopierbare Programme handelt. Diese gefährlichen digitalen Waffen können selbst aus halbwegs engagierten Einzelpersonen mächtige Angreifer ganzer Wirtschaftssysteme machen. Im Falle von WannaCry ist die Weltwirtschaft nur wegen der diletantischen Programmierung, von einem katastrophalen Schaden bewahrt worden. Aus diesen Gründen scheint seit wenigen Tagen der US-amerikanische Nachrichtendienst NSA seine Veröffentlichungspraxis zu ändern.

Die in Deutschland durch die Gründung des BSI bisher angestrebte Trennung von Schutz der Bevölkerung und der Entwicklung von digitalen Angriffswaffen hat zu einer im Vergleich zu anderen Staaten höheren Vertrauensbildung geführt. Ausdrücklich lobend erwähnt sei die vertrauensbildende Arbeit des BSI im Falle Huawei. Diese hat im Bereiche der aufziehenden Handelskrieges zu einer Deeskalation beigetragen. Dieses Vertrauen sollte in einer immer instabileren Weltlage nicht aufs Spiel gesetzt werden, sondern gepflegt, ausgebaut und auch institunell verstetigt werden.

- Das Nichtschließen von Sicherheitslücken bedroht angesichts der weiter fortschreitenden Vernetzung in den Bereichen Industrie und der kritischen Infrastruktur nicht mehr nur im digitalen Sinne Heimat und innere Sicherheit.

Übersicht

In dieser Stellungnahme soll der Einsatz von Kryptographie von der mathematischen und der informatischen Sicht diskutiert werden. Im weiteren Text werden, nach einer Analyse der Bedrohungslage mit einen Schwerpunkt auf die konkreten Gefahren für die innere Sicherheit durch die fortschreitende Vernetzung von Industrie und kritischer Infrastruktur, Handlungsempfehlungen insbesondere im Bereich der Open Source Software gegeben.

Kryptographie als Gestaltungsmittel

Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingestzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder für jeden Engagierten brechbar ist. Diese Eigenschaft verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten. Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergerführt, erweitert und intelligent verstetigt werden.

Grundlagenforschung Kryptographie und Systemdesign

Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitererführt, erweitert und intelligent verstetigt werden.

Post-Quantum Kryptographie zwingend notwendig

- Mathematischen Grundlagenforschung im Bereich der Post-Quantum-Kryptographie ist die einzige praktische Herangehensweise für mittel bis langfristige sichere Verschlüsselung und Signierung.

Systemrelevante Open-Source Softwareprojekte

Die genannten Open-Source Projekte stellen systemrelevante Sicherheitssoftware für den Erhalt der digitalen Souveränität dar. Eine nachhaltige Sicherung dieser Projekte ist wichtig für die digitale Souveränität und damit auch Aufgabe staatlicher Stellen. Aufgrund der vielen ehrenamtlichen Projektteilnehmer sind die entstehenden Kosten gering. Die Offenen Lizenzen garantieren die Nachhaltigkeit

- VeraCrypt: Festplattenverschlüsselung

Firmengeheimnisse und andere vertrauliche Daten sollten immer verschlüsselt gespeichert werden – vor allem, auf mobilen Geräten, die leicht gestohlen werden können. Das früher vielfach genutzte Truecrypt wird offiziell nicht mehr weiterentwickelt, aber die offene Lizenz erlaubte eine Weiterentwicklung unter dem Namen Veracrypt.

- Open SSH: Kommunikations-Sicherheit

Open SSH dient unter anderem der abhör- und fälschungssicheren Übermittlung von Steuerinformationen an eingebettete Systeme oder Internetserver.

- Open SSL: Datentransport-Sicherheit

TLS (Transport Layer Security) ist das im Internet am meisten genutzte Sicherheitsprotokoll. Leider gibt es immer wieder Sicherheitslücken im TLS-Protokoll, oder in einzelnen TLS-Bibliotheken. Open SSL ist die meistgenutzte und deshalb wichtigste TLS-Bibliothek.

- GNU Privacy Guard: Anwendungs-Sicherheit

Der GNU Privacy Guard wurde zum Versenden von verschlüsselten und unterschriebenen E-Mails nach dem Open PGP Standard entwickelt. GnuPG ist auch wichtig, um die Herkunft und Echtheit von Sicherheitsupdates zu überprüfen.

- Das TOR Projekt: Anonym Surfen

Mit Hilfe des TOR-Browsers kann man im Netz surfen, ohne seine Identität zu verraten. Das TOR Projekt wird momentan vorwiegend vom US Verteidigungsministerium finanziert.

Anmerkungen zur Pflicht zur Herausgabe von Passwörtern in § 15 TMG Entwurf

Zur Diskussion des Spannungsverhältnis zwischen Entwurf TMG und der DGSVO sei aus der Stellungnahme der Digitalen Gesellschaft e.V. an das Bundesministerium der Justiz und für Verbraucherschutz zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität zitiert.

> "Die Bestimmung in § 15a TMG n.F. umfasst dem Wortlaut nach eine Pflicht zu Herausgabe von Passwörtern. Zum einen ist nicht ersichtlich, welchen legitimen Nutzen die Herausgabe von Passwörtern für die Strafverfolgungsbehörden haben kann. Sofern bestimmte Informationen, die auf einem Account gespeichert sein könnten, von Interesse für die Strafverfolgung sind, können diese herausverlangt werden. Ob der Erhalt von Passwörtern etwa zum verdeckten Weiterbetrieb eines Accounts durch Behörden führen soll, für den keine Rechtsgrundlage ersichtlich ist, oder zum Ausprobieren für andere Accounts der betreffenden Person – solche denkbaren Verwendungen der Passwörter wären verfassungswidrig. Passwörter dürfen nach der DSGVO nicht im Klartext gespeichert werden, um Integrität und Vertraulichkeit zu gewährleisten. Gespeichert sind demnach bei Anbietern, die ihre datenschutzrechtlichen Pflichten einhalten, in der Regel Hashwerte von Passwörtern, mittels derer ermittelt werden kann, ob ein eingegebenes Passwort richtig ist, die jedoch nicht auf das Passwort als solches zurückgerechnet werden können. Deshalb stellt sich auch die Frage der Vereinbarkeit der vorgeschlagenen Regelung mit europäischem Datenschutzrecht."

Änderung einer Zahl macht Passwortermittlung unmöglich

Auch an diesem Beispiel kann man einfach die Macht von kryptographischen Lösungen erkennen. Das kryptographische Modell geht von der praxisnahen Annahme aus, daß ein Angreifer zumindest lesenden Zugriff auf die Zugangsinformationsdatei erhält.

Sichere Speicherung von Zugangsinformationen

Das gängigste Verfahren zur Anmeldung bei Internetdiensten ist die Verwendung der Kombination Nutzername und Passwort. Es ist unmittelbar nachvollziehbar, daß eine Datei, die Nutzernamen und Passwörter im Klartext enthält für Angreifer ein sehr lohnendes Ziel wäre.

- Die Kenntnis des Inhaltes dieser einen Passwortdatei würde das gesamte Zugriffssystem komplett kompoimitieren. Aus diesem Grund ist es eine strikte Anforderung der Sicherheitsforschung stattdessen nur einen Wert zu Speichern, welcher durch Verwendung einer Einwegfunktion (in der Praxis durch kollissionsresitente Hashfunktionen realisiert) auf das Passwort und einem zusätzlichen Zufallswert (Salt) berechnet wird. Andere Vorgehensweise entsprechen nicht dem Stand der Technik sind sind somit zum Bearbeiten von persönlichen Daten nicht rechtskonform.

- DGSVO treue Anbieter besitzen keine gespeicherten Passwörter.

Wiederholungszähler

Um dem Angreifer trotz der Kenntnis der Zugangsdatei das Errechnen der eigentliche Passworte zu erschweren, verwendet man in der Praxis vereinfacht gesprochen meist einen Zähler, welcher das Berechnen der Einwegfunktion durch mehrfache Ausführung schwerer macht. Setzt man diesen DGSVO-konform auf den Stand der Technik, können auch Ermittlungsbehörden die gewünschten Passworte nicht mit vertretbarem Aufwand bestimmen.

Für Mathematiker und Forscher im Bereiche der IT-Sicherheit ist es eine sehr spannende Beobachtung, daß die lange Zeit als zu theoretisch und paranoid kritisierten Sicherheitsmodelle die realistischste Einschätzung der aktuellen Sicherheitslage darstellen.

Akademisches Sicherheitsmodell

Bei der Analyse der Sicherheit von Computernetzwerken geht man in der theoretischen Modellbildung von sehr mächtigen Angreifern aus, die alle Nachrichten mitlesen und verändern kann. Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingesetzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder faktisch für jeden Engagierten brechbar ist. Aus diesem Grunde verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten.

Praktisches Sicherheitsmodell

- Siehe letzten Abschnitt.

Auch aus rein technischer Sicht zeigt die Tatsache, dass gespeicherte Daten in der real existierenden IT-Welt (2020) nicht gesichert werden können, die Notwendigkeit eines verfassungsrechtlichen Schutzes.

- Grundannahme: Jeder Technische Schutz für Daten versagt eines Tages.

Generelle Hackbarkeit

Bedeutend für eine gesellschaftliche Einschätzung ist auch die Tatsache, dass neben den Diensten fremder Staaten auch Privatpersonen und Firmen in der Praxis recht einfach (in der Regel rechtswidrigen) Zugriff auf die heutigen Computersysteme erlangen können. Es haben sich hier Online-Marktplätze für ausnutzbare Sicherheitslücken (Zero-Days) gebildet, an denen sich in rechtlich problematischer Weise auch deutsche Dienste beteiligen. Die Preise sind schwankend, allerdings meist für Einzelpersonen mit höhere Einkommen und kleinere Firmen durchaus finanzierbar. Inzwischen gibt es bereits frei

verfügbare Werkzeuge, die nur geringe Anforderungen an die Computerkenntnisse des Angreifers stellen.

Cyberwaffen sind kopierbar

Die Ausnutzung von Sicherheitslücken hat die Eigenschaft, dass die Angriffswerkzeuge kopierbare Programme sind. Diese gefährlichen digitalen Waffen können selbst aus halbwegs engagierten Einzelpersonen mächtige Angreifer ganzer Wirtschaftssysteme machen. Im Falle von WannaCry ist die Weltwirtschaft nur wegen der diletantischen Programmierung, von einem katastrophalen Schaden bewahrt worden. Aus diesen Gründen scheint seit wenigen Tagen der US-amerikanische Nachrichtendienst NSA seine Veröffentlichungspraxis zu ändern.

Die in Deutschland durch die Gründung des BSI bisher angestrebte Trennung von Schutz der Bevölkerung und der Entwicklung von digitalen Angriffswaffen hat zu einer im Vergleich zu anderen Staaten höheren Vertrauensbildung geführt. Ausdrücklich lobend erwähnt sei die vertrauensbildende Arbeit des BSI im Falle Huawei. Diese hat im Bereiche der aufziehenden Handelskrieges zu einer Deeskalation beigetragen. Dieses Vertrauen sollte in einer immer instabileren Weltlage nicht aufs Spiel gesetzt werden, sondern gepflegt, ausgebaut und auch institutionell verstetigt werden.

- Das Nichtschließen von Sicherheitslücken bedroht angesichts der weiter fortschreitenden Vernetzung in den Bereichen Industrie und der kritischen Infrastruktur nicht mehr nur im digitalen Sinne Heimat und innere Sicherheit.

Sicherheitsproblem Industrievernetzung: Gefahren über die Digitale Welt hinaus

Die Sicherheitslage ist im Bereich des Internet-of-Things (IoT) aus einer Reihe von Gründen deutlich schlechter als in der klassischen Computerindustrie. Viele Geräte adressieren einen Markt mit sehr geringen Stückpreisen oftmals im einstelligen Eurobereich. Ein organisiertes Netzsicherheitsmanagement, welches die PC-Industrie über viele Jahre mit erheblichem Aufwand aufbaute, ist im Massenanlagenbau meist nicht zu finden. Oftmals bestehen nicht einmal ausreichende Update-Möglichkeiten. Verschärft wird dies durch eine im niedrigpreisigen Gerätemarkt geringere Kundenbindung der Hersteller, so dass die Verbraucher nicht befriedigend über nötige Sicherheitsupdates informiert werden. Weiterhin haben viele eingebettete Systeme eine weit längere Einsatzzeit als persönliche Computersysteme. Diese kann beispielsweise bei smarten Heizungssteuerungen viele Jahre betragen. Schließlich ist auch bei vielen Verbrauchern oft nicht einmal das Wissen vorhanden, dass das wegen seiner Funktion angeschaffte Gerät einen wartungsintensiven Internet-Teilnehmer darstellt.

Industriesteuerungen

Von unsicheren IoT Geräten gehen Gefahren nicht nur für die digitale Welt aus. So können Störungen in industriellen Anlagen Katastrophen auslösen. Auch innerhalb der Hausvernetzungen liegen etwa bei der Heizungssteuerung nicht zu unterschätzende Gefahrenpotentiale vor. Zahlreiche Autoren demonstrierten, wie Angreifer bestimmte IoT-Geräte dazu bringen können, eine Infektion durch ein Schadprogramm weiterzugeben. Innerhalb weniger Minuten können sich Zehntausende von ungeschützten IoT-Geräten in einer Stadt zu einem einzigen, von den Angreifern kontrollierten Botnetz zusammenschließen.

Haftung für Schäden

Die seit geraumer Zeit vermehrt auftretenden Angriffe mit Millionen übernommener IoT Geräte zeigen eine neue Dimension des Problems. Für den Verbraucher entsteht unter anderem auch das Problem, dass mit übernommenen Geräten angerichtete Schäden die IP-Adresse des Besitzers als Angriff-

sherkunft hinterlassen. Dies kann sowohl juristische Folgen, als auch Folgen für die technischen Systeme haben. Abwehrmaßnahmen der angegriffenen Systeme können zu Störungen der unwissend für Angriffe missbrauchten IoT Systemen führen.

- Aus Sicht des Verbraucherschutzes ist eine Klärung der Haftung für von IoT Geräten verursachte Schäden und eine stärkere Inverantwortungnahme der Hersteller herbeizuführen.
- Umgekehrt muss von Verbrauchern verlangt werden, dass Sie für Geräte, die die Sicherheit der Allgemeinheit gefährden, die Verantwortung übernehmen und zumindest die Sicherheitsupdates der Hersteller auch einspielen, so es welche gibt.

Sicherheitsupdates und Nachhaltigkeit

Die Erfahrung der letzten Jahre lehrt, dass alle Kommunikationsgeräte zu einer Gefahr für ihre Nutzer und für die Allgemeinheit werden können, wenn nicht regelmäßig entdeckte Sicherheitslücken durch Sicherheitsupdates geschlossen werden. Ein wichtiger Grundsatz ist deshalb, dass während der gesamten Lebenszeit eines Gerätes Sicherheitsupdates geschrieben und installiert werden müssen. Eingebettete und IoT Geräte sind da keine Ausnahme. In der Praxis ist die Einhaltung dieses Grundsatzes ein Problem. Erstens haben die Hersteller, wenn sie ihre Geräte einmal verkauft haben, oft kein ökonomisches Interesse an einer weiteren Pflege und dem Erstellen vom Sicherheitsupdates. Zweitens ist, vor allem bei kleinen Herstellern, nicht klar, wie lange dieser Hersteller am Markt sein wird, bzw. wie lange es eine verantwortliche Firma gibt, die Sicherheitsupdates erstellen kann. Um dieses Problem zu lösen, schlagen wir das Folgende vor.

Handlungsvorschläge IoT-Sicherheit

- Hersteller sind während der gesamten Lebenszeit eines IoT Gerätes dazu verpflichtet, Sicherheitsupdates zu schreiben und an die Nutzer zu verbreiten.

- Wollen die Hersteller sich, nach Ablauf einer angegebenen Lebenszeit, dieser Verpflichtung entziehen, müssen sie spätestens zu diesem Zeitpunkt ihre Quelltexte als Open-Source veröffentlichen. Damit soll sichergestellt werden, dass zumindest Dritte das Schreiben und ggf. Verbreiten von Sicherheitsupdates übernehmen können.

- Soweit die Quelltexte der Hersteller anfänglich nicht Open-Source sind, müssen sie bei einem Treuhänder hinterlegt werden. Kommt ein Hersteller den genannten Verpflichtungen nicht nach oder existiert der Hersteller nicht mehr, sorgt der Treuhänder für die Veröffentlichung der Quelltexte als Open-Source.

Die Notwendigkeit der Datensparsamkeit

Beginnend mit dem Volkszählungsurteil des Bundesverfassungsgerichts (1983) hat sich in Deutschland ein weltweit beachtetes Datenschutzrecht in Gesetzgebung und Rechtsprechung entwickelt. Datensparsamkeit ist die verfassungsrechtlich und höchstrichterlich geforderte einzuhaltende Norm.

Datenverzicht

Heute müssen sich Datenschutzexperten daher auch in hoch konfliktäre Diskussionen einbringen. Das hier leider vorherrschende politische Diskussionsklima schreckt dabei verständlicherweise viele Wissenschaftler ab. Dennoch gebietet es die gesellschaftliche Verantwortung, darauf hinzuweisen, wenn technische Entwicklungen, wie eine allumfassende Überwachung oder die praktische Angreifbarkeit von Computersystemen, juristische Datenschutzsicherungen praktisch unwirksam werden lassen. In der Computer-Sicherheitsforschung herrscht die Meinung vor, dass Daten auf vernetzten Computersystemen generell als hackbar anzusehen sind.

- Wenn man nicht bereit ist, das Risiko einer möglichen Veröffentlichung von vertraulichen Daten einzugehen, darf man die Daten gar nicht erst speichern.

Daten von besonders gefährdeten Personengruppen

Wer Daten speichert, oder eine Verpflichtung zum Speichern bestimmter Daten einführt, muss die Vorteile, die sich aus einer Speicherung ergeben, mit den Nachteilen, die sich aus einer Veröffentlichung der Daten ergeben würden, abwägen – selbst wenn eine Veröffentlichung der Daten nicht vorgesehen ist. Es genügt keinesfalls, die Daten nur rechtlich zu sichern (also, ihre Veröffentlichung zu verbieten bzw. unter Strafe zu stellen). Es genügt nicht einmal, die Daten, zusätzlich zu dem juristischen Schutz auch technisch zu schützen, mit Maßnahmen, die dem Stand der Technik entsprechen. Denn nicht einmal die Kombination von rechtlichen und technischen Sicherungsmaßnahmen gibt eine Garantie dafür, dass die Daten auf Dauer geheim bleiben. Erwachsen aus einer möglichen Veröffentlichung besonders schwere Nachteile für die Betroffenen, oder sogar eine Gefahr für Leib und Leben, müssen die Vorteile einer Speicherung diesen Nachteilen und Gefahren gegenübergestellt werden.

Geschlossene Systeme und Systemsicherheit

Die Frage, ob geschlossene oder offene Systeme hinsichtlich der Systemsicherheit vorzuziehen sind, ist zentral innerhalb der Informatik. Während geschlossene Systeme im günstigen Falle durch eine ausreichende Qualitätskontrolle einige Angriffe verhindern können, ist, falls die Qualitätskontrolle versagt, der Schaden vom Nutzer selbst nur schwer abwehrbar. Neben der Trusted Computing Infrastruktur verbaut Intel in zahlreichen seiner Prozessoren eine eigene Sicherheitsarchitektur. Diese ist ein geschlossenes Konzept, welches höchst problematische Eigenschaften aufweist. Daher ist eine grundsätzliche Deaktivierung der Intel Active Management Technology (AMT) zu empfehlen.

Alternative Vertrauensanker

Es ist zwingend notwendig, Alternativen zum Vertrauensanker von Microsoft zur Verfügung zu stellen. Aus technischen Gründen ist dies sogar deswegen notwendig, weil Microsoft teilweise mit einer Schlüssellänge von 2048 bit arbeitet, welche vom BSI nicht für langfristige Sicherheit empfohlen wird.

- Für den staatlichen Bereich könnte beispielsweise die Bundesnetzagentur eine führende Position einnehmen. Hier sind im Zusammenhang mit dem Signaturgesetz schon erhebliche Vorarbeiten vorgenommen worden.

- Für nichtstaatliche Bereiche erscheint eine gemeinnützige Stiftung außerhalb der USA die bessere Lösung. Als Beispiele könnten hier die Reformen bei ICANN und das verteilte Erzeugen von DNSSEC-Rootzonenschlüssel dienen.

Quellenhinweis

Teile dieser Stellungnahme enthalten aktualisierte Vorschläge und Analysen, welche im Rahmen der Studie

- Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen der Bundesministeriums für Justiz und Verbraucherschutz
- Juni 2017
- Technologien für und wider Digitale Souveränität
- Rüdiger Weis, Stefan Lucks, Volker Grassmuck
- `https://www.svr-verbraucherfragen.de/wp-content/uploads/Weis_Lucks_Grassmuck_Studie_.pdf`

erstellt und veröffentlicht wurden. Diese fachübergreifende Studie enthält weitere Empfehlungen, Analysen der Auswirkung der Digitalisierung und ein ausführliches Quellenverzeichnis und sei zur zusätzlichen Lektüre empfohlen.