VERBAND DER INTERNETWIRTSCHAFT E.V.

Positionspapier zur

Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - JOIN(2017) 450 final

Berlin/Brüssel, 18. Dezember 2017

Am 13. September 2017 stellte die Europäische Kommission zusammen mit dem Hohen Vertreter der EU für Außen- und Sicherheitspolitik ihre neue Cyber-Sicherheitsstrategie vor. Mit der Strategie sollen die Eckpfeiler für die zukünftige Politik der EU im Bereich der Sicherheit für IT-Systeme und deren Vernetzung festgeschrieben werden.

Neben der Stärkung der Resilienz gegen Angriffe auf IT-Systeme wird auch der institutionelle Rahmen auf europäischer Ebene, insbesondere die Europäische IT-Sicherheitsagentur ENISA, näher beleuchtet. Die Schaffung eines europäischen Binnenmarkts für Cybersicherheit wird adressiert und die Umsetzung der NIS-Richtlinie als Eckpunkt festgeschrieben.

Die diskutierten Maßnahmen sind für die Internetwirtschaft relevant. Sie betreffen Dienste und Produkte, die in ihren Netzwerken und Rechenzentren betrieben werden. Sie sind maßgeblich für den Regulierungsrahmen im Bereich der Cybersicherheit und für die Funktionsfähigkeit von Netzen und Diensten. Gleichzeitig gilt es sicherzustellen, dass der Rechtsrahmen für Cybersicherheit so gestaltet wird, dass alle Marktteilnehmer, Behörden, Nutzer, Diensteanbieter und Netzbetreiber einen Rechtsrahmen bekommen, der gegenseitiges Vertrauen ebenso berücksichtigt, wie ökonomische Notwendigkeiten.

I. Zentrale Aspekte einer europäischen IT-Sicherheitspolitik

Die IT-Sicherheitspolitik der Europäischen Union sollte idealerweise komplementär mit der ihrer Mitgliedsstaaten sein. Dort wurden bereits in verschiedenen Bereichen nationale Regelungen geschaffen. Auch besteht bereits für digitale Dienste ein bewährter rechtlicher Rahmen, den es zu berücksichtigen gilt. Gleichzeitig sollte eine europäische IT-Sicherheitspolitik auch - genau wie der europäische Binnenmarkt - kohärent ausgestaltet sein. Eine Fragmentierung der IT-Sicherheitsregeln wäre ebenso wie deren Dopplung kontraproduktiv und würde der Verwirklichung der EU-Cyber-Sicherheitsstrategie zuwiderlaufen.

Folgende Aspekte sollten daher bei der weiteren Umsetzung der europäischen IT-Sicherheitspolitik maßgeblich sein:

- **IT-Sicherheit vernetzt denken**

Immer wieder wird diskutiert, ob Regierungen oder Ermittlungsbehörden Zugang zu Kommunikationsinhalten oder Verbindungsdaten bekommen sollen. Neben Maßnahmen wie einer Verpflichtung zur Speicherung solcher Daten werden dabei auch Maßnahmen wie die Bereitstellung einer zentralen Schnittstelle für das Auslesen von Daten, ein zentraler Master Key für die Entschlüsselung von Kommunikation oder das Ausnutzen von Schwachstellen in IT-Produkten diskutiert. eco hält alle diese Maßnahmen für nicht zielführend, wenn es darum geht, sichere und vernetzte Kommunikationssysteme zu schaffen und zu gestalten. Alle schwächen digitale Kommunikation aller Teilnehmer und die Integrität digitaler Systeme. Gerade in einer vernetzten Welt kann dies Folgen haben, die weit über die unmittelbar betroffenen Dienste hinausgehen. Pauschale Maßnahmen lehnt eco deshalb ab und fordert stattdessen Kooperation bei der Absicherung digitaler Systeme.

- **Digitale Fürsorgepflicht des Staates ernst nehmen**

Die Internetwirtschaft wird beim Thema IT-Sicherheit in die Pflicht genommen. Das NIS-Richtlinien-Umsetzungsgesetz, das IT-Sicherheitsgesetz, die NIS-Richtlinie, die geplante ENISA-Verordnung und weitere Sicherheitsmaßnahmen definieren hierfür z.T. sehr hohe Anforderungen an Unternehmen. Dabei darf es jedoch nicht bleiben. Auch der Staat steht in der Verantwortung. Staatliche Stellen und Sicherheitsbehörden sollten ebenso dazu verpflichtet sein, erkannte Sicherheitslücken zu melden, um eine breite Gefährdung von Nutzerinnen und Nutzern auszuschließen.

- **Vielfalt digitaler Dienste erhalten - pauschale Regulierung vermeiden**

Digitale Dienste sind nach wie vor Innovationstreiber. Die Vielfalt, mit der Daten genutzt und verwendet werden, spiegelt die Vielfalt der Dienste wieder, die derzeit auf dem Markt verfügbar sind. Diese Vielfalt gilt es auch bei der Definition von Sicherheitsauflagen zu berücksichtigen. Eine pauschale und zentrale Regulierung für all diese Dienste hält eco für nicht zielführend und hilfreich - ebenso wie eine gesonderte Regulierung für digitale Dienste. Generelle Regelungen sollten dort zum Tragen kommen, wo sie Sinn ergeben. Anpassungen bestehender Regelungen an digitale Herausforderungen sollten sorgfältig geprüft werden. Dies gilt insbesondere bei den Planungen von Gütesiegeln und deren Rahmen.

- **Rechtsrahmen der e-Commerce Richtlinie bewahren**

Die e-Commerce Richtlinie hat klare Auflagen für Provider geschaffen, wie sie mit rechtswidrigen Inhalten umzugehen haben. Dies gilt auch bei Auflagen für die Durchsuchung von Plattformen. Diese Maßstäbe haben auch im Rahmen einer europäischen Cyber-Sicherheitspolitik ihre Gültigkeit

und sollten daher unbedingt berücksichtigt werden. Sie durch Auflagen zur Produktgestaltung oder den Zugriffswunsch von Sicherheitsbehörden zu unterlaufen, hält eco für schädlich.

- **Vertrauen von Nutzern angemessen berücksichtigen**

Nahezu überall kommen heute vernetzte Geräte zum Einsatz. Smartphones, Tablets, Fitnessarmbänder und Haushaltsgeräte stellen Dienste bereit und tauschen Daten aus. Nutzer haben Vertrauen in die bereitgestellten Dienste und müssen auch imstande sein, deren Sicherheit angemessen beurteilen zu können. Vor diesem Hintergrund zeigt sich immer wieder, dass ein einfacher, niedrigschwelliger Ansatz gewählt wird, der Nutzer und Unternehmen gleichermaßen Informiert und einfache Hilfestellungen leistet. Pauschale Warnsysteme oder starre Bekanntmachung oder Eingriffe in Netzwerke und Systeme helfen nicht dabei, Vertrauen zu schaffen und die Sicherheit zu verbessern. Die Diskussion über weitere Maßnahmen sollten stets im Kontext des europäischen digitalen Binnenmarkts geführt werden.

II. Zur EU-Cyber-Sicherheitsstrategie im Einzelnen:

Die EU-Cyber-Sicherheitsstrategie erläutert die Eckpfeiler der einzelnen Maßnahmen. eco sieht an verschiedenen Stellen noch weiteren Erörterungs- und Klärungsbedarf, die im Zuge der Umsetzung der einzelnen Maßnahmen angegangen werden sollten. Konkret zu folgenden Punkten:

- **Zu 2.1 „Strengthening the European Union Agency for Network and Information Security“**

ENISA hat lange ein Schattendasein geführt und trat als europäischer Akteur und Gestalter nur bedingt auf. Bisherige Schwerpunkte der Agentur waren Informationsveranstaltungen und Handreichungen zum Thema IT-Sicherheit. Mit dem mittlerweile ebenfalls vorgestellten Entwurf der ENISA-Verordnung (COM(2017) 477 final/2) sollen die Aufgaben der Agentur nun neu festgeschrieben werden. Die Stärkung der Beraterrolle von ENISA im Bereich der Entwicklung von Cyber-Sicherheitspolitik begrüßt eco im Sinne eines ganzheitlicheren Ansatzes im Bereich der Absicherung von IT-Systemen und Netzwerken. Insbesondere die Schnittstellenfunktion für die Initiativen in den verschiedenen Sektoren kann hier für die gesamte Wirtschaft hilfreich sein. Die ebenfalls geplanten „Information Sharing and Analysis Centres“, die für zentrale Wirtschaftsbereiche geplant sind, bieten zudem die Möglichkeit, Sicherheit als vernetztes Gestaltungsfeld zu begreifen und entsprechend gemeinsame Lösungen für zentrale Probleme zu entwickeln.

Die zukünftige Rolle von ENISA bei der Zertifizierung von IT-Produkten hängt aber stark davon ab, wie der institutionelle Rahmen hierfür gestaltet wird und inwieweit es ENISA gelingt, tatsächlich praktikable Vorschläge an die Europäische Kommission und das Europäische Parlament heranzutragen

und diese dann auch davon zu überzeugen. Als die europäische Organisation, welche das Faktenwissen und die Kenntnisse der Attacken besitzt, ist sie dafür prädestiniert. Bei der Rollenausgestaltung wird aber auch darauf zu achten sein, dass vorhandene nationale Kompetenzen in einem stringenten organisatorischen Gefüge im Sinne einer kooperativen Zusammenarbeit eingebracht werden können.

- **Zu 2.2 „Towards a Single Cybersecurity Market“**

Die Europäische Kommission hat sich die Schaffung eines digitalen Binnenmarkts zum Ziel gesetzt. In zahlreichen Feldern hat sie dem bereits Rechnung getragen. Es ist daher nur konsequent und nachvollziehbar, wenn auch Anstrengungen unternommen werden, dies für den Themenkomplex der IT-Sicherheit nachzuvollziehen.

Irritierend ist an den Plänen der Kommission für einen Cyber-Sicherheits-Binnenmarkt allerdings, dass sie hier den zuvor beschrittenen Weg der kooperativen Zusammenarbeit verlässt, den sie im ENISA-Kapitel vorgezeichnet hat. Sie stellt stattdessen einen Zertifizierungsrahmen für den Themenkomplex in den Mittelpunkt ihrer Überlegungen. Das auf drei Säulen basierende Zertifizierungssystem, das die Kommission zur Debatte stellt, soll augenscheinlich einen Binnenmarkt durch zentrale Vorgaben für Cybersicherheit gestalten - ein Ansatz, der große Risiken in sich birgt. Mögen die hohen Sicherheitsauflagen für kritische und stark risikobehaftete IT-Systeme noch nachvollziehbar sein, so sollten Hersteller von „weit verbreiteten digitalen Produkten, Netzwerken, Systemen und Diensten, die im privaten wie im öffentlichen [nicht kritischen] Bereich zu Einsatz kommen“ eher gefordert sein, ihre Produkte möglichst sicher zu entwickeln, um Schwachstellen zu minimieren und das Angriffsrisiko mit Hilfe von Orientierung bietenden Schutzprofilen und branchen- oder produktspezifischen Standards zu senken. Pauschale, nicht differenzierende Auflagen für IT-Systeme sind eher kontraproduktiv. Es besteht das Risiko der Schaffung von Silos, welche dann durch die Erfüllung von Auflagen für „sicher“ erklärt werden und konterkarieren dadurch die Vernetzung sowie das Zusammenwachsen von Diensten im Netz. Pauschale Regelungen helfen nicht dabei, IT-Sicherheit zu verbessern. Stattdessen könnte unter Berücksichtigung der Kritikalität der verarbeiteten Daten, bzw. der Anwendung an sich, eine sachgerechte Skalierung nach möglichem Schadensausmaß und Eintrittswahrscheinlichkeit oder nach geeigneten Widerstandsklassen erfolgen. Die Skalierung sollte demnach vorwiegend dazu dienen, die Transparenz zu erhöhe, bzw. um als Anwender eine valide Risikoeinschätzung durchführen zu können.

Vor diesem Hintergrund ist die Ankündigung der EU-Kommission bis Juni 2018 Haftungsregelungen im Bereich der IT-Sicherheit überprüfen zu wollen, intensiver zu beleuchten. Prohibitiv hohe Sicherheitsauflagen in Verbindung mit scharfen Produkthaftungsregeln sind für die vernetzte Gesellschaft und deren Dienste kritisch zu betrachten. Zwar ist anzuerkennen, dass die EU-Kommission zugesteht, dass kein Produkt zu 100 Prozent sicher sein kann,

dennoch bleibt das Problem bestehen, dass die Pläne der EU sich schädlich auf digitale Dienste und Produkte auswirken können - insbesondere auf die in der EU ansässigen Unternehmen. Überlegungen zu einer weiteren Gestaltung der Herstellerhaftung im IT-Bereich sollten daher unter diesem Aspekt mit Vorsicht getätigt werden.

Die exemplarische Auflistung „spezifischer Sektoren“, die dazu aufgefordert werden, ihre eigenen Strategien einzubringen, deutet auch an, dass dann zusätzlich zu den pauschal hohen Sicherheitsauflagen noch weitere, branchenspezifische Standards hinzukommen, was die Lage und Auflagen für Anbieter, Netzbetreiber und Softwareentwickler zusätzlich erschwert. Dies gilt umso mehr bei Anwendungen, die verhältnismäßig offen und dementsprechend auch flexibel einsetzbar sind. Auch die Überprüfung des direkten Investments aus dem Ausland in europäische Schlüsseltechnologien wird den Spielraum für Unternehmen und Produkte erheblich einschränken, da ein Screening auch den Eingriff in Investitionen quasi vorwegnimmt.

Positiv hervorzuheben ist allerdings, dass die Kommission die Bemühungen Dritter würdigt, die hilfreiche Beiträge zur Verbesserung von Cybersicherheit liefern können.

- **Zu 2.3 Implementing the Directive on the Security of Network and Information Systems in full**

Die NIS-Richtlinie stellt seit 2016 den rechtlichen Rahmen für die IT-Sicherheit in Europa dar. Sie unterwirft Unternehmen und Diensteanbieter einer Meldepflicht. Ihre Umsetzung stellt einen weiteren Eckpfeiler der EU-Cyber-Sicherheitsstrategie dar. Die EU möchte hierfür Leitlinien für eine gemeinsame Implementierung vorlegen. Inwieweit dies für Deutschland relevant sein wird, bleibt abzuwarten. Die Umsetzung ist hier bereits weit fortgeschritten. Die von der Kommission angekündigten Handreichungen zu best-practices können sich als hilfreich für die Staaten erweisen, die bis jetzt noch keine Maßnahmen ergriffen haben. Die Implementierung der NIS-Richtlinie sollte in allen EU-Mitgliedsstaaten dringend forciert werden, da schon jetzt absehbar ist, dass diese noch vor Ablauf der Umsetzungsfrist veraltet sein wird. Eine mittel- bis langfristige Novellierung sollte daher nach der Umsetzung ebenfalls geprüft werden. Im Zuge einer Novellierung wären bspw. eine systematische Betrachtung der gesamten Wertschöpfungskette denkbar, um adäquate Maßnahmen zu ergreifen und das Schutzniveau v.a. kritischer Infrastrukturen signifikant zu erhöhen.

- **Zu 2.4 Resilience through rapid emergency response**

Um den Auswirkungen großangelegter Cyberattacken im digitalen Binnenmarkt besser begegnen zu können, ist eine Einbeziehung europäischer Institutionen sinnvoll - zum einen, da sich deren Institutionen vor Angriffen selbst schützen müssen, zum anderen, da die räumlichen Auswirkungen von Cyberangriffen auch an Staatsgrenzen nicht zwangsläufig

haltmachen. Der Aufbau eigener Kompetenzen und Kapazitäten zur Bewältigung von Sicherheitslagen ist daher sinnvoll und nachvollziehbar. Der „Blueprint“ für Cyber-Sicherheitsvorfälle gibt konkrete Handlungsanleitungen. Der zusätzlich geplante „Cybersecurity Emergency Response Fund“ kann dabei helfen, die entstandenen Schäden zu bereinigen und stellt hierfür konkrete Mittel zur Verfügung. Beides ist aus Sicht des eco im Sinne einer verantwortungsvollen Vorsorge begrüßenswert. In diesem Kontext ist aber auch festzuhalten, dass Informationstransparenz zentral ist und daher auch staatliche Stellen und insbesondere Sicherheitsbehörden entdeckte Sicherheitslücken melden müssen, so dass diese schnellstmöglich geschlossen werden können.

- **Zu 2.5 A cybersecurity competence network with a European Cybersecurity Research and Competence Centre**

Zur Gestaltung von IT-Sicherheit gehört auch, dass Informationen über Sicherheitslücken und Bedrohungen vertrauensvoll ausgetauscht werden können und Instrumente zu deren Schließung bzw. Beseitigung entwickelt werden. Der von der EU hier angeregte Weg eines Netzwerks öffentlicher Forschungsprogramme und -mittel bietet Potential für eine bedarfsbezogene und anwendungsorientierte Forschung - sofern es gelingt, Internetwirtschaft und die IT-Industrie angemessen mit einzubeziehen. Eine primär oder rein akademisch orientierte Cyber-Sicherheitsforschung wäre weniger effektiv. Dies gilt es, bei den weiteren Schritten hin zu dem von der EU geplanten Netzwerk zu berücksichtigen.

- **Zu 2.6 Building a strong EU cyber skills base**

Die Bemühungen der EU bei der Entwicklung und Stärkung der Bildung in digitalen Themen deckt sich eng mit den zentralen Forderungen des eco in diesem Bereich. Neben der Stärkung der Kompetenzen von Arbeitskräften und akademischen Ausbildungen sollte hierbei auch die Schulbildung berücksichtigt werden, die die Grundlage für den Erwerb und die weitere Spezialisierung von Fachwissen darstellt. Zentral für den Erfolg dieser Maßnahmen ist der Entwicklung konkreter Maßnahmen und die angemessene Ausstattung von Bildungseinrichtungen mit entsprechender Technologie. Ein ähnlich umfassender Zugang zu Bildungseinrichtungen sollte gelegt werden, um die Grundlage zu schaffen, mehr IT-Sicherheits-Experten auszubilden. In diesem Kontext ist auch der spezifische Kompetenzausbau im Hochschulumfeld notwendig.

- **Zu 2.7 Promoting cyber hygiene and awareness**

Ebenfalls positiv konnotiert sind die geplanten Maßnahmen der EU bei der Sensibilisierung von Bürgerinnen und Bürgern. Ein zentrales europäisches Portal für Tools und weitere Maßnahmen kann bestehenden Aktivitäten mehr Resonanz verleihen und diese positiven Beispiele für IT-Sicherheitslösungen

Bürgerinnen und Bürgern zugänglich machen. Je besser sich diese gegen Gefahren selbst absichern und diese einschätzen können, desto eher kann Vertrauen in digitale Dienste entstehen und deren Akzeptanz verbreitert werden. Die Stärkung von IT-Sicherheit beim e-Government begrüßt eco daher ebenso. Der Ausbau und die konkrete Ausgestaltung des Rahmens für elektronische Identitätsnachweise sollte dabei möglichst offen gestaltet werden und damit innovationsorientiert erfolgen. Die Schärfung des Bewusstseins für IT-Sicherheitsprobleme aber auch den verantwortungsvollen Umgang mit Medien hält eco für zentral. Sie sind gegenüber den Versuchen, das austarierte Haftungsgefüge der e-Commerce Richtlinie auszuhöhlen, vorzuziehen, da sie den verantwortungsvollen und wertebezogenen Umgang mit Medien Rechnung tragen, statt diesen der Technologie und ihren Möglichkeiten zu unterwerfen. Der in der Strategie enthaltene Appell an die Internetwirtschaft wird von eco in diesem Sinne gesehen.

- **Zu 3.1 Identifying malicious actors**

Die Identifizierung von Straftätern und deren Verfolgung ist ein verständliches Ziel. Daher ist es nachvollziehbar, wenn die Europäische Kommission eine Aufstockung der Ressourcen zur Bekämpfung von Cybercrime fordert und damit auch Europol gestärkt werden soll. Die Stärkung von Ermittlungsbehörden ist aus Sicht von eco grundsätzlich ein richtiger Schritt. Vor allem für kleine EU-Mitgliedsstaaten können zusätzliche Kapazitäten auf europäischer Ebene Entlastung bringen. Gleichzeitig gilt es darauf zu achten, dass insbesondere bei zusätzlichen Kompetenzen und neuen Regeln die Verantwortung nicht auf private Akteure und die Internetwirtschaft abgewälzt werden. Auch darf keine Konstellation entstehen, bei der Diensteanbieter pauschal für Vergehen von Nutzern in Haftung genommen werden. Das Herkunftslandsprinzip und die jeweilige nationale Rechtsordnung müssen dabei ebenfalls beachtet werden.

Zur besseren Identifizierung von Straftätern erhofft sich die EU-Kommission u.a. ein beschleunigtes Ausrollen der IPv6 Adressen, damit Nutzer leichter identifizierbar sind. Mitgliedsstaaten sollen dazu freiwillige Vereinbarungen mit den Providern treffen. Der Gedanke, dem diese Überlegung zu Grunde liegt, ist aus Sicht von eco datenschutzrechtlich nicht unproblematisch. Deshalb sollte bei den freiwilligen Vereinbarungen darauf geachtet werden, dass durch die Umsetzung von IPv6 das Vertrauen in Dienste und Produkte nicht geschmälert wird. In diesem Kontext sollte auch darauf geachtet werden, dass WHOIS-Anfragen, die ebenfalls neugestaltet werden sollen, Registrare nicht mit übermäßigen Auflagen zu belegen und auch hier den Datenschutz zu berücksichtigen.

- **Zu 3.2 Stepping up the law enforcement response**

Um Kriminalität effektiv grenzübergreifend zu bekämpfen sieht die Europäische Kommission die Notwendigkeit, den grenzüberschreitenden

Zugriff auf mögliche elektronische Beweismittel, so genannte e-Evidence, zu erleichtern. Überlegungen dazu hat sie bereits in einem Inception Impact Assessment vorgestellt. Die Überlegungen der Kommission sind nicht zielführend, da sie nicht an den Stellen ansetzen, die regelmäßig zu Problemen in der Beweissicherung in internationalen Ermittlungen führen. Stattdessen stellen sie eine stärkere Inanspruchnahme von Dienstanbietern in Aussicht und hebeln rechtsstaatliche Prinzipien und bewährte rechtskonforme Prozesse in den Mitgliedsstaaten aus. Auch die angekündigte Überprüfung der Bedeutung von Verschlüsselung bei der Strafverfolgung ist vor diesem Hintergrund kritisch zu bewerten. Zwar wird nicht ausdrücklich eine zentrale Schnittstelle oder Backdoor gefordert, die eco aus Sicherheitsgründen und Gründen der Vertraulichkeit heraus ablehnt. Gleichwohl stehen die im Papier dargelegten Überlegungen zum Einsatz von IuK-Technologie durch Kriminelle dieser Forderung nach solchen Maßnahmen, die der Sicherheit abträglich wären, nicht völlig entgegen.

Auch bei der Überprüfung der Rolle der EU beim Übereinkommen über Computerkriminalität gilt es, Rechtssicherheit für Anbieter von Telekommunikations- und Telemediendiensten zu bewahren. Bereits jetzt sind die Maßnahmen, die die Konvention gestattet, sehr weitgehend und es ist fragwürdig, inwieweit sie überhaupt mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in Einklang zu bringen sind.

Die Ankündigung der Kommission, mehr Ressourcen in die effektive Bekämpfung von Cyberkriminalität zu investieren, begrüßt eco.

- **Zu 3.3 Public-private cooperation against cybercrime**

Öffentlich-private Partnerschaften werden bereits verschiedentlich zur Realisierung von IT-Sicherheit genutzt. Die von der EU ins Leben gerufene European Cyber Security Organization (ECSO) ist ein Beispiel für eine mögliche Institutionelle Ausgestaltung, ebenso wie das in dem Bericht der Kommission erwähnte G4C e.V. unter Beteiligung von BKA und BSI. Die Europäische Kommission wünscht sich, dass solche öffentlich-privaten Partnerschaften verstärkt dort zum Einsatz kommen, wo traditionelle Mechanismen der Polizeiarbeit versagen. Dieses Ansinnen ist, wie bereits bei der Debatte um e-Evidence zu erkennen war, hochproblematisch, da sie augenscheinlich dazu dienen können, rechtsstaatliche Prinzipien auszuhöhlen und die Verantwortung des Staates und seiner Sicherheitsbehörden auf private Unternehmen und Akteure abzuwälzen. Das untergräbt das Vertrauen von Nutzerinnen und Nutzern in digitale Technologien und in Institutionen. Den Preis für diese Politik zahlen Bürgerinnen und Bürger.