Cybersicherheit & Sicherheitstechnologien

Bitkom-Position zur Bundestagswahl 2021

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Sebastian Artz | Bereichsleiter Cyber- & Informationssicherheit
T 030 27576-206 | s.artz@bitkom.org

Titelbild

© Henk Mohabier – pexels.com

Wo wir stehen & was wir wollen

Die Sicherheit von Informationstechnologien entscheidet wesentlich über den Erfolg, die Strahlkraft sowie die digitale Souveränität des Wirtschaftsstandorts Deutschland. Deshalb ist die nächste Bundesregierung angehalten, die IT- und Cybersicherheit als einen politischen Schwerpunkt zu etablieren und die vielen bestehenden Fehlausrichtungen im Bereich der Cybersicherheit zu korrigieren.

Gelingen kann dies nur, wenn die Gestaltungskraft, die der Zusammenarbeit zwischen Staat und Wirtschaft innewohnt, zur Entfaltung gebracht wird. Denn die Wirtschaft ist weit mehr als bloßer Produktlieferant. Die Wirtschaft leistet als Innovationsgarant, Know-how-Träger und Ausbilder unverzichtbare Beiträge zur Gemeinschaftsaufgabe Cybersicherheit. Dies wird aber nur bedingt anerkannt. In Deutschland mangelt es an einer politischen Diskussion darüber, wie der Staat Wirtschaft und Bevölkerung im Cyberraum schützen kann.

Was es konkret braucht, ist eine zielgerichtete, risiko- und evidenzbasierte sowie auf die Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) ausgerichtete Cybersicherheitspolitik, in der das Wissen sowie die Erfahrungen und Bedarfe der Wirtschaft, der Wissenschaft und der Zivilgesellschaft entsprechend Gehör und Berücksichtigung finden. Neben dem offenen und ehrlichen Dialog mit der Wirtschaft fordert Bitkom dazu in der kommenden Legislaturperiode mehr Tatkraft auf allen Ebenen, damit Deutschland digital endlich aufholt. Die Verringerung des digitalen Hinterherhinkens kann aber nur gelingen, wenn mit der Digitalisierung zeitgleich Maßnahmen zur echten und wirksamen Erhöhung der Cybersicherheit strukturiert auf den Weg gebracht und umgesetzt werden. Nur so ist eine sichere Nutzung digitaler Dienste und Technologien durch Staat, Wirtschaft und Bevölkerung zu erreichen. Zudem gilt es, die Cybersicherheitspolitik europäischer auszurichten und konstruktiv auf die EU-Initiativen einzuwirken.

Handlungsempfehlungen für die neue Legislaturperiode

- **Cybersicherheit als Hebel zur Stärkung souveränen Handelns begreifen:** Auf die in der repräsentativen Bitkom-Unternehmensumfrage zur 'Digitalen Souveränität 2021' gestellte Frage »In welche Technologien sollte Deutschland jetzt investieren, um technologisch unabhängiger zu werden?« landete die Antwortoption IT-Sicherheitstechnologien mit 96 % ganz vorne auf dem 1. Platz und damit weit vor Technologien wie Robotik, IoT, autonomen Fahren oder Cloud Computing. Die Stärkung und strategische Nutzung unseres bereits exzellenten IT-Sicherheitsstandorts sowie die existierende und vertrauensvolle Zusammenarbeit mit unseren europäischen und internationalen Partnern in Wirtschaft, Wissenschaft und Zivilgesellschaft muss Kernanliegen der kommenden Legislaturperiode sein.

  - **Deutschlands künftige Exportschlager müssen Cybersicherheit als zentralen Wesenszug in sich tragen:** Im Bereich der Cybersicherheit ist ein Paradigmenwechsel erforderlich. Bis heute wird Cybersicherheit vielfach noch als Add-on der (End-)Produktentwicklung gesehen. Dies muss sich ändern. Die Sicherheit von Schlüssel- und Zukunftstechnologien muss im Sinne eines »Security by Design«-Ansatzes von vornherein mitgedacht und gestärkt werden. Das gilt nicht nur für Hersteller von Softwareprodukten oder digitalen Diensten, sondern auch für Endgeräte. Es gilt sicherzustellen, dass jeder Teil der Wertschöpfungskette einen Beitrag zur Gewährleistung von Cybersicherheit leistet und die regulierte Verantwortung nicht nur einigen Stakeholdern zugeschrieben wird. Gerade mit Blick auf die immer größer werdende Vernetzung (u. a. IoT) und steigende Zahl an Endgeräten braucht es zusätzlich einen stärkeren Fokus auf das Thema Cybersicherheit – die Wahl eines Gerätes und/oder einer Anwendung muss zunehmend zu einer Sicherheitsentscheidung werden. Daneben sollte Security by Design auch für E-Government-Lösungen und Verwaltungshandeln gemäß einem risikobasierten Ansatz gelten und sich im Regulierungsrahmen konsequent widerspiegeln. Zudem können insbesondere E-Government- und Verwaltungslösungen vom Zusammenspiel aus Open Source und Open Development profitieren. Anstelle einer fehlgeleiteten, reinen Versteifung auf freien Quellcode kann die gemeinsame Entwicklung mit der Community operationalisierte Transparenz schaffen und dadurch echte Mehrwerte in puncto Cybersicherheit generieren.

  - **Bildung als Schlüssel zum Erfolg verstehen:** Eine wesentliche Komponente sowohl von digitaler Souveränität als auch von Cybersicherheit ist die zukunftsfähige Bildung aller Menschen in Deutschland. Der Wandel von einer Industrie- zu einer Informationsgesellschaft ist im vollen Gange, allerdings ohne dass die Bildung Schritt hält. Für eine gesunde Informationsgesellschaft müssen Medienkompetenz und IT-Know-how spätestens ab der Grunschule in die Bildungspläne integriert werden. Es braucht nicht weniger als einen Paradigmenwechsel in der schulischen, universitären und beruflichen Aus- und Weiterbildung. Die Kurrikula müssen umgebaut und Cybersicherheitskurse alters- und leistungsgerecht in allen schulischen, universitären und beruflichen Aus- und Weiterbildungsangeboten integriert werden. Informatik ist als Pflichtfach ab Sekundarstufe I einzuführen. Darüber hinaus sind die

jungen Talente von heute und morgen maßgeblich auf politischen Lösungspragmatismus angewiesen. Statt maximaler Risikoaversion und tausendfacher, langwieriger Einzelprüfungen durch häufig selbst hilfesuchende Betroffene – bspw. Lehrkräfte beim schulischen Einsatz von Videokonferenzlösungen – muss im Kontext des jeweiligen Anwendungsfalls viel stärker in Richtung pauschaler Risikobewertung gedacht werden, die dann allgemeingültig für ganz Deutschland anwendbar ist. Letzteres gilt nicht nur im Bereich Bildung, aber vor allem dort.

- **Dem Fachkräftemangel entgegenwirken – insbesondere durch Frauenförderung:** Dem Mangel an Fach- und Führungskräften in der IT-Branche generell und insb. im Bereich der Cybersicherheit muss dringend begegnet werden. Zur Abmilderung des strukturellen Mangels muss das Potenzial der gesellschaftlichen Vielfalt genutzt und vor allem die Förderung von Frauen gestärkt werden. Es besteht dringender Bedarf an mehr weiblicher Beteiligung in der Cybersicherheitsbranche. Es braucht Empowerment, Anreize, Förderprogramme und Vorbilder auf allen Stufen eines persönlichen Karrierewegs – beginnend spätestens ab der Grundschule. Gleichzeitig braucht es die Entwicklung neuer Angebote für Quereinsteigende und deren Verankerung im Programm der Bundesagentur für Arbeit. Bitkom fordert einen Online-Weiterbildungsmonitor, der Jobsuchenden, Arbeitnehmenden und Arbeitgebern niedrigschwellig Informationen zu Weiterbildungsbedarf und -möglichkeiten bietet. Zudem sollten Anreize für Unternehmen geschaffen werden, um technisches und fachliches Know-how an die Jugend weiterzugeben und mehr Interesse an IT- und Cybersicherheitsberufen sowie -ausbildungen zu wecken. Hierzu bedarf es intensivierter Kooperationen zwischen Unternehmen und Ausbildungsinstituten.

- **»Usability« von Sicherheit stärker in den Blick nehmen – von der Anwendungs- bis zur Infrastrukturebene:** Die in der Gesellschaft beobachtbare und sogar zunehmende Diskrepanz zwischen Sicherheitswissen und Sicherheitsverhalten muss nicht nur politisch thematisiert, sondern auch in einem konkreten Maßnahmenplan umgesetzt werden. Zur Schließung der Wissens-Verhaltens-Schere ist die Anwenderfreundlichkeit von Sicherheitslösungen, die in Gesellschaft, Wirtschaft und Verwaltung zum Einsatz kommen, zu incentivieren – bspw. in Vergabeverfahren. Dabei lohnt auch ein verstärkter Fokus auf »Digital Nudging« – also auf Maßnahmen, die erwünschtes Sicherheitsverhalten einfach und attraktiv machen. Zur tatsächlichen Zielerreichung muss sich der Usability-Gedanke aber auch auf der Infrastrukturseite widerspiegeln. Dies bedeutet, gleichzeitig Wege zu finden, digitale »state-of-the-art«-Dienste entsprechend zu entwickeln und nutzbar zu machen – bspw. für sichere und hochperformante Cloudlösungen.

- **Mittelstand mitdenken:** KMU sind meist auf externe Hilfe angewiesen und verfügen nicht über eigene Ressourcen, um notwendige Cybersicherheitsvorkehrungen zu treffen. Die kommende Bundesregierung muss sich fragen: Was ist uns der Schutz des Mittelstands wert und welche gesellschaftlichen Kosten sind auf lange Sicht höher? Auf diese Fragen braucht es ernsthafte politische Antworten. Neben der Bereitstellung qualitativ hochwertiger und praxisnaher Informations- sowie Unterstützungsangebote, bspw. durch die Allianz für Cyber-

sicherheit, das Cyber-Sicherheitsnetzwerk oder die Transferstelle IT-Sicherheit im Mittelstand (TISiM), fordert Bitkom steuerliche Anreize, um Kostensynergien zu nutzen und den Einsatz von Cybersicherheitslösungen für KMU attraktiver zu machen. In Übereinstimmung mit dem BSI empfiehlt Bitkom 20 % des IT-Budgets in Cybersicherheit zu investieren.

- **Wirtschaftsschutz stärken:** Angesichts der sich zuspitzenden Bedrohungslage, nicht zuletzt durch die hohe Anzahl an Ransomware-Angriffen, müssen Staat und Privatwirtschaft zielorientiert zusammenarbeiten. Was es braucht, ist ein ganzheitlicher Ansatz zur Stärkung des Wirtschaftsschutzes und zum Aufbau notwendiger Cyberresilienz. Dies erfordert einen intensiveren Austausch aller Beteiligten. Insbesondere KMU, aber auch große Unternehmen, Forschungseinrichtungen und Behörden auf allen politischen Ebenen, können davon nur profitieren. Der Informationsaustausch zwischen Staat, Wirtschaft und Wissenschaft zur Threat Landscape, Incidence Response und Vulnerability Disclosure ist auszubauen und weiter zu institutionalisieren.

- **Geheimschutz weiterentwickeln:** Geheimschutzbetreute Unternehmen leisten einen unverzichtbaren Beitrag zur Aufrechterhaltung essenzieller Fähigkeiten in sicherheitssensiblen Bereichen. Für die Unternehmen müssen planbare Innovationsprozesse und Vorgaben geschaffen werden, um Geheimschutz sicher, praktikabel und modern auszurichten. Deshalb bedarf es einer Aktualisierung des Geheimschutzhandbuchs und einer höheren Priorisierung von Geheimschutzfragen im politischen Raum.

- **Verbindliche Sicherheitsanforderungen bei öffentlichen Beschaffungen festlegen:** Es gibt eine große Lücke zwischen Sicherheitspolitik und Beschaffungspraxis. In der Beschaffung liegt der Schwerpunkt oft nach wie vor auf dem Preis. Die öffentliche Hand ist mit Abstand der größte Beschaffer im Land und sollte sich für höhere Cybersicherheitsstandards und eine Weiterentwicklung der Vergabekriterien bei der öffentlichen Beschaffung einsetzen. Bei allen Digitalisierungsprojekten ist eine Mindestquote für Investitionen in Cybersicherheit vorzusehen. Eine Orientierung an den bereits oben genannten 20 % erscheint sinnvoll.

- **Behördliche Eigenentwicklungen nicht als Allheilmittel begreifen:** Es sei ausdrücklich auf die Risiken hingewiesen, die mit der Tendenz hin zu behördlichen Eigenentwicklungen einhergehen. Nachvollziehbare Beweggründe dürfen nicht in kostenintensiven Sackgassen münden und zu Konkurrenzsituationen mit Unternehmen führen.

- **Starke, vertrauenswürdige Verschlüsselungstechnologien für mehr Cybersicherheit garantieren:** Neben staatlichen Institutionen ist es vor allem die hochinnovative, wissensgetriebene und häufig international orientierte deutsche Wirtschaft, die sich auf sichere, kryptografische Methoden verlassen können muss. In Anbetracht der Tatsache, dass Cybersicherheit nur durch wirksame Verschlüsselung gewährleistet werden kann, braucht es – wie in der *Grundsatzerklärung des Bitkom zur Verschlüsselung*[1] aufgezeigt – ein klares Verbot, den Cyberraum staatlicherseits zu schwächen.

  - **Globale Strahlkraft des Standorts Deutschland für die Cybersicherheit verinnerlichen:** Die Beschaffenheit des Cyberraums impliziert, dass nationale Handlungen grenzüberschreitende Auswirkungen haben und entsprechende Signalwirkung entfalten. Wie in der UN-Resolution *A/RES/73/266*[2] dargelegt, bedarf es des verantwortlichen Handelns von Staaten im Cyberraum. Dieser Verantwortung muss sich Deutschland in der heutigen Zeit mehr denn je bewusst sein und die Vorreiterrolle annehmen. Die kommende Bundesregierung muss deshalb klar und gemeinsam mit den europäischen Partnern definieren, was ihre Schutzziele im Cyberraum sind und welche gesetzgeberischen Maßnahmen konkret auf welche Schutzziele einzahlen.

  - **Effizient funktionierendes Schwachstellenmanagement etablieren:** Es muss eine Meldepflicht für entdeckte Sicherheitslücken gelten – auch und insb. für staatliche Stellen. Ein spezifisches Vulnerability Management muss in Abstimmung mit einer neutral agierenden Institution erfolgen und einem standardisierten Responsible Disclosure-Verfahren mit den Herstellern folgen, damit die Patch-Erstellung und -Verteilung an die Kunden klar geregelt wird. In einem solch transparenten und eindeutig geregelten Rahmen sind dann auch haftungsrechtliche Verpflichtungen denkbar, um die schnellstmögliche Schließung von Schwachstellen zu gewährleisten. Die politische Adressierung haftungsrechtlicher Verpflichtungen wird vom Bitkom grundsätzlich unterstützt, muss aber zwingendermaßen gemeinsam und im Einvernehmen mit der Wirtschaft erfolgen – allein schon, um die Komplexität der Lieferketten und Produktlebenszyklen adäquat zu berücksichtigen. Notwendige Grundvoraussetzung für ein derartiges und effizient funktionierendes Schwachstellenmanagement auf allen Produktebenen ist ein Vertrauensverhältnis von Wirtschaft und staatlichen Institutionen, welches es aufzubauen und zu pflegen gilt.

  - **Verschlüsselungstechnologien und Krypto-Agilität zur Priorität erklären:** Mit der rasant voranschreitenden Entwicklung von Quantencomputern steigt die Notwendigkeit, Post-Quanten-Kryptografie zu nutzen. Die Entwicklung zukunftssicherer Verschlüsselungsverfahren muss daher Hand in Hand gehen mit staatlichen Förderbestrebungen, um die flächendeckende Migration zu Quantencomputer-resistenten Infrastrukturen in Wirtschaft und Verwaltung zu bewerkstelligen.

1 ↗ https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsatzerklarung-verschlusselung.pdf

2 ↗ https://digitallibrary.un.org/record/1658328

- **Regulatorische Komplexitätsreduktion umsetzen:** Komplexität ist der größte Feind von Sicherheit. Was auf technischer Ebene gilt, gilt einmal mehr auf regulatorisch-administrativer Ebene. Mehr Cybersicherheit wird nicht durch gesetzgeberisches Mikromanagement erreicht. Gleiches gilt mit Blick auf die Cybersicherheitsarchitektur und die unübersichtliche Zuständigkeitsstruktur auf Bundes- und Länderebene. Je früher die Verantwortungsdiffusion angegangen wird, desto geringer die Kollateralschäden für Wirtschaft, Wissenschaft und Gesellschaft. Daher sollten die Zuständigkeitsstrukturen vereinfacht und verschlankt und die Kompetenzen in wenigen Händen gebündelt werden. Hierbei gilt es auch, auf Verwaltungs- wie auf Unternehmensseite die Silos zwischen Cybersicherheit und Wirtschaftsschutz zu überwinden und Sicherheit ganzheitlich zu denken – auch organisatorisch.

- **Die Stärkung des digitalen europäischen Binnenmarkts zur Vorbedingung aller Vorhaben machen:** In einem starken, innovativen und zukunftsgerichteten Europa muss Cybersicherheit global, mindestens aber europäisch, gedacht werden. Andernfalls würden selbst gut gemeinte Maßnahmen als Sammelsurium nationaler Alleingänge ohne signifikante Steigerung des Sicherheitsniveaus ins Leere laufen. Bitkom fordert EU-weit harmonisierte und sich an internationalen Standards orientierende Cybersicherheitsvorschriften für Technologieprodukte, einheitliche Prüf- und Zertifizierungsvorgaben auf EU-Ebene sowie eine tragfähige Cybersicherheitsarchitektur. Konkret denkbar wäre bspw. die Erweiterung des CE-Kennzeichens um Cybersicherheitsanforderungen. EU-weit harmonisierte IT-Sicherheitsvorschriften für Produkte und Infrastrukturen stärken den digitalen Binnenmarkt, der – wie oben ausgeführt – globale Strahlkraft zur Erhöhung der IT- und Cybersicherheit entfalten kann. Die IT-Sicherheitsvorschriften sollten dabei immer zusammen mit der Wirtschaft entwickelt und bestehende Zertifizierungen zu fairen Bedingungen erneuert und gegenseitig anerkannt werden. Zwischen neuen Zertifizierungssystemen und bestehenden wie Common Criteria sollte eine gegenseitige Anerkennung oder Entsprechung hergestellt werden.

- **Kritische Infrastrukturen wirksam schützen:** Mit dem IT-Sicherheitsgesetz (IT-SiG) 2.0 hat die Bundesregierung die Vorgaben für Betreiber kritischer Infrastrukturen aktualisiert und Unternehmen im besonderen öffentlichen Interesse neu reguliert. Bitkom steht Maßgaben, die einen echten Schutz der öffentlichen Sicherheit bewirken, offen gegenüber. Die künftige Bundesregierung muss sich für eine enge Anlehnung der NIS2-Richtlinie auf europäischer Ebene an das deutsche IT-SiG 2.0 einsetzen und daran mitwirken, dass die NIS2 harmonisiert umgesetzt wird. Ständig wechselnde Vorgaben für Unternehmen erzeugen große Unsicherheit und wirken dem eigentlichen Ziel entgegen. Es müssen langfristig planbare Verhältnisse geschaffen werden.

- **Gemeinsame Feedbackschleifen aktiv nutzen:** Nach den gemachten negativen Erfahrungen im Zuge des Entstehungsprozesses des IT-SiG 2.0 fordert Bitkom die frühzeitige, regelmäßige und enge Einbindung bei der Erarbeitung künftiger Gesetzesvorhaben, insb. natürlich beim IT-SiG 3.0, sowie die gesetzgeberische Berücksichtigung des eingebrachten Feedbacks. Die vorausschauenden und partizipativen Konsultationsprozesse der Europäischen Kommis-

sion zur Erarbeitung der NIS2-Richtlinie sollten auch national zum Standard werden und angemessene Kommentierungsfristen von mindestens vier Wochen vorsehen. Zugleich muss glaubhaft erkennbar sein, dass den zuständigen Ressorts ausreichend Zeit zur Verfügung steht, die Änderungsbedarfe umzusetzen. Zeit darf kein limitierender Faktor für gute und sicherheitssteigernde Gesetzgebung sein. Zu diesem Zwecke fordert Bitkom die konsequente Nutzung und Bereitstellung von Synopsen im Entstehungsprozess künftiger Gesetzesvorhaben. Dies erleichtert nicht nur den Kommentierungsprozess, sondern dient auch als unmittelbare Hilfestellung für den Gesetzgeber bei der Entwicklung von Gesetzesänderungen. Darüber hinaus wäre eine zentrale Koordinationsfunktion im Rang eines Staatsministers oder Staatssekretärs ein wesentlicher Meilenstein – nicht nur für gesetzgeberische Konsultationsprozesse.

- **Bedarfsgerechtigkeit staatlicher Regulierung berücksichtigen:** Die Bewertung der Notwendigkeit von Cybersicherheitsregulierung muss immer den tatsächlichen Regulierungsbedarf sowie die Angemessenheit und praktische Effektivität eines staatlichen Eingriffs berücksichtigen. Es muss genau evaluiert werden, wo tatsächlich Bedrohungslagen bestehen oder konkret absehbar sind und ob staatliches Handeln in bestimmten Bereichen der Cybersicherheit auch wirklich zum gewünschten Ergebnis führen.

- **Offene staatliche Fehlerkultur zulassen:** Das staats- und behördenzentrierte Cybersicherheitsverständnis bedarf einer viel stärkeren incentivierenden Haltung im Sinne der Idee des Vorlebens. Staatliche Stellen sollten mit positivem Beispiel vorangehen und insb. KMU signalisieren: »Schaut, wir schaffen es auch« – bspw. indem Kommunen auf ein ordentliches Sicherheitsniveau angehoben werden. Dazu gehört auch, Selbstkritik zulassen. Etablierte Unternehmen und Branchen, die bereits den Sprung zu einem hohen Grad an Cybersicherheit erreicht haben, leisten in einem solchen Szenario ihren Beitrag, in dem sie aktiv hinzugezogen werden und ihre Erfahrungen und ihr Wissen teilen.

- **IT-Sicherheitskennzeichen digitalisieren:** Bei der Entwicklung von IT-Sicherheitskennzeichen sollten Hersteller die Möglichkeit haben, ihre Produkte wahlweise physisch oder elektronisch zu kennzeichnen. Die Vorteile von E-Labels sind: gezielte und leichter zugängliche Informationen für die jeweilige Zielgruppe; einfachere Informationsaktualisierung; positive Auswirkungen auf die Umwelt; weniger regulatorische Belastungen für Produktinnovationen; verbesserte Rückverfolgbarkeit und Transparenz von Produkten (Marktüberwachung); leichterer Nachweis der Einhaltung von Vorschriften.

- **Gesamtgesellschaftliche Informationsbasis zur Cyberbedrohungslage aufbauen und Meldewesen vereinfachen:** Das große Potenzial der Bereitstellung von Echtzeitinformationen muss endlich genutzt werden, um die Reaktionsfähigkeit auf aktuelle und drohende Cybersicherheitsbedrohungen zu verbessern – idealerweise EU-weit. Dazu braucht es eine zentrale Anlaufstelle zur Information über Cybersicherheitsbedrohungen und -vorfälle. Diese zentrale Anlaufstelle ist eng mit dem oben skizzierten und noch aufzubauenden Schwachstellenmanagement zu verzahnen. Im Zuge des Aufbaus einer solchen leuchtturmartigen

Anlaufstelle ließe sich auch endlich die bisherige Einbahnstraße der Meldungen über IT-Sicherheitsvorfälle in ein Modell zum beiderseitigen Nutzen weiterentwickeln. Anstelle reiner PDF-Berichte fordert Bitkom ein leicht verständliches Dashboard mit klar definierten Gefahrenindikatoren, maschinenlesbare Datensätze und entsprechende Schnittstellen (APIs), die eine Auswertung in Echtzeit ermöglichen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org