Digitale Souveränität: Einschätzungen in der deutschen Wirtschaft und Verwaltung

Ergebnisse einer repräsentativen Umfrage des Analystenhauses techconsult im Auftrag von LANCOM Systems, Mai 2015

techconsult
The IT Market Analysts

LANCOM
Systems

LANCOM Systems

Inhaltsverzeichnis

LANCOM Systems

Zusammenfassung

In der vorliegenden Untersuchung wurden 411 Entscheider aus Unternehmen unterschiedlicher Branchen, Verwaltung und NGOs in Deutschland zu ihrer Einschätzung und Einstellung in Bezug auf Digitale Souveränität befragt. Die zentralen Ergebnisse im Überblick:

Digitale Souveränität ist eine der dringendsten netzpolitischen Aufgaben

- Die Politik hat noch keine Antwort darauf gefunden, wie sie die Digitale Souveränität Deutschlands und Europas stärken kann.

- Backdoors in IT-Produkten werden als Gefahr für die Digitale Souveränität angesehen.

- Digitale Souveränität ist zukunftsweisend. Sie wird als eine wesentliche Voraussetzung für die erfolgreiche Digitalisierung von Produktionsprozessen (Industrie 4.0) und für eine sichere Nutzung von Cloud-Diensten angesehen.

- Es wird eine Vielzahl an Maßnahmen befürwortet, um die Digitale Souveränität zu stärken, darunter die Aufnahme von Vertrauenswürdigkeitskriterien bei der Vergabe von öffentlichen Aufträgen, gezielte Sicherheitsüberprüfungen ausländischer IT-Produkte oder die Prüfung der Vertrauenswürdigkeit von IT-Komponenten durch nationale oder europäische Stellen. Technisch gesehen können ein sicherer Transportweg für die Datenübertragung und eine konsequente Ende-zu-Ende-Verschlüsselung ganz wesentlich zu mehr Digitaler Souveränität beitragen. Generell ist die Politik gefordert, die Basis für Digitale Souveränität zu schaffen: Mit verlässlichen rechtlichen Rahmenbedingungen, einheitlichen Datenschutzrichtlinien, verbindlichen Mindeststandards, einer konsequenten Industriepolitik oder einer strategisch angelegten ITK-Innovationspolitik.

Vertrauensbildende Maßnahmen sind dringend erforderlich

- Vertrauliche und sensible Daten – sei es von Bürgern, Unternehmen oder Behörden und staatlichen Einrichtungen – werden heute als nicht ausreichend geschützt empfunden.

- Das Vertrauen in den BND ist stark erschüttert, er genießt von allen deutschen Einrichtungen das geringste Vertrauen. Das Vertrauen in die Bundesregierung hat ebenfalls gelitten.

- Die Vertrauenswürdigkeit des Anbieters ist neben Sicherheit ein zentrales Kriterium, auf das bei der Wahl von IT-Lösungen ein besonderes Augenmerk gelegt werden sollte.

1. Methode

Der deutsche Marktanalyst techconsult hat die Online-Umfrage „Einschätzungen zur Digitalen Souveränität“ im Auftrag von LANCOM Systems im Mai 2015 durchgeführt. Die 411 Teilnehmer aus unterschiedlichen Branchen wurden über eine Online-Befragung adressiert.

Zunächst wurden die Branchen, in denen die Befragten tätig sind und die Unternehmensgröße abgefragt. Es folgten Fragen zur Position im Unternehmen, zum Alter, Geschlecht, Bundesland und zur IT-Kompetenz (Selbsteinschätzung).

Der Fragebogen bestand aus neun inhaltlichen Fragen rund um das Thema Sicherheit und Bedrohungen im Internet. Die zentralen Umfrageblöcke bildeten die Themen Vertrauen und Digitale Souveränität.

2. Demographie

Branchen:

Von den 411 Teilnehmern sind 152 im Dienstleistungsbereich, 97 in der Industrie (inkl. Baugewerbe) beschäftigt, 63 in Öffentlichen Verwaltungen bzw. Non-Profit-Organisationen, 49 im Handel, 32 in Banken und Versicherungen, 10 in der Telekommunikation, 8 in der Energie- und Wasserversorgung.

Unternehmensgröße:

110 Teilnehmer arbeiten in Unternehmen mit weniger als 50 Mitarbeitern. 103 Befragte sind in Unternehmen mit 50 bis unter 500 Mitarbeitern tätig, 93 Teilnehmer arbeiten in Unternehmen mit 500 bis unter 1.000 Mitarbeitern. 105 Befragte sind Unternehmen mit 1.000 und mehr Mitarbeitern zuzuordnen.

Position:

101 befragte Personen sind Inhaber, Geschäftsleiter oder Geschäftsführer. Das obere Management war mit 70 Teilnehmern an der Umfrage vertreten. Es beteiligten sich 129 Bereichs- und Abteilungsleiter an der Befragung sowie 111 Leitende Mitarbeiter.

Alter:

18 Personen waren unter 30 Jahre alt, 96 Personen zwischen 30 und 40 Jahren. Mit 127 Teilnehmern bei den 40- bis 50-Jährigen und 133 Teilnehmern bei den 50- bis 60-jährigen waren diese beiden Altersgruppen am stärksten vertreten. Es beteiligten sich darüber hinaus 37 Personen der Alterskategorie über 60 Jahre an der Umfrage.

Geschlecht:

Von den 411 Teilnehmern der Umfrage waren 96 weiblich und 315 männlich.

IT-Kompetenz:

74 Teilnehmer schätzen ihre IT-Kompetenz als sehr groß ein, 236 als groß. 89 der Befragten geben an, dass sie eine geringe IT-Kompetenz haben und 12 Personen halten diese für sehr gering.

3. Ausgangslage

Am 12. Mai veröffentlichte der BITKOM sein Positionspapier zur Digitalen Souveränität, in dem er mehr Unabhängigkeit bei der Nutzung digitaler Technologien für Deutschland und Europa fordert. Es ist nicht zuletzt eine Konsequenz der Snowden-Enthüllungen, die uns in den vergangenen zwei Jahren vor Augen geführt haben, in welchem Maße wir von ausländischen IT-Angeboten abhängig sind und welche Folgen dies für unsere digitale Selbstbestimmung und die Kontrolle über unsere digitalen Infrastrukturen hat.

Neben dem BITKOM plädieren Vertreter aus Politik und Wirtschaft seit Bekanntwerden der NSA-Ausspähaktivitäten verstärkt für mehr Digitale Souveränität und machen sich für die Rückeroberung der Kontrolle über die digitalen Infrastrukturen stark.

Doch wie steht es zwei Jahre nach den ersten Snowden-Enthüllungen tatsächlich um die digitale Selbstbestimmung Europas? Deutschland und Europa sind weiterhin stark auf ausländische IT-Lösungen angewiesen. Gerade diesen wird aber heute nur wenig Vertrauen entgegengebracht.

Vernetzte Produktion, Industrie 4.0, das Internet der Dinge, die Cloud – all das sind Trends, die der deutschen Wirtschaft in den kommenden Jahren einen neuen Schub geben sollen. Sind sie möglich ohne eine vertrauenswürdige, sichere Infrastrukturbasis? Ohne vertrauenswürdige, sichere Netze?

Dem Thema Vertrauenswürdigkeit kommt ohne Frage eine zentrale Rolle zu, denn für eine digital souveräne Gemeinschaft ist ein vertrauensvolles Miteinander unabdingbar. Der durch die Snowden-Enthüllungen entstandene Vertrauensverlust war sicherlich der Ausgangspunkt für die gesamte Debatte um die „Digitale Souveränität".

Die Vertrauensfrage lässt sich auf fast alle Ebenen projizieren. Vertrauen wir unserer Regierung, dass sie uns und unsere Daten im digitalen Zeitalter bestmöglich schützt? Vertrauen wir den Unternehmen, mit denen wir in einer geschäftlichen Beziehung stehen? Vertrauen wir den Herstellern der IT-Lösungen, die wir nutzen, dass sie ihre Produkte nur zu unserem Nutzen konzipiert haben?

Es geht also nicht nur um Sicherheit, es geht um Vertrauenswürdigkeit. Und um die Frage, ob ein Produkt ganz nebenbei Hintertüren, die sogenannten Backdoors, offenhält für den einen oder anderen Dienst, der sich ungestört in unseren Netzen umsehen kann.

Die aktuelle Studie, die vom deutschen Marktanalysten techconsult im Auftrag von LANCOM Systems im Mai 2015 in Deutschland durchgeführt wurde, gibt Auskunft darüber, wie Vertreter aus dem oberen und mittleren Management in Deutschland die Lage einschätzen, welche Bedeutung das Thema Vertrauen für sie in diesem Kontext hat und wie sie zur Forderung nach mehr Digitaler Souveränität stehen.

4. Ergebnisse

4.1 Einschätzung des Gefahrenpotentials im Internet

Neben der zentralen Frage nach der Digitalen Souveränität ging die Studie den Fragen nach, wie gut die Teilnehmer über IT-Sicherheit Bescheid wissen, inwieweit sie sich der Risiken für ihr Unternehmen bewusst sind, ob ihr Unternehmen bereits selbst Opfer eines Angriffs geworden ist und welche Bedrohungen sie besonders fürchten.

4.1.1 Persönlicher Informationsstand bezüglich IT-Sicherheit

Fast 66 Prozent der Befragten schätzen ihren Informationsstand bezüglich IT-Sicherheit als groß oder sehr groß ein. Knapp 31 Prozent geben an, dass sie diesen für gering halten. Am besten informiert fühlt sich das obere Management – hier beurteilen 81,5 Prozent ihren Informationsstand zu IT-Sicherheit als groß oder sehr groß. Bezogen auf die Unternehmensgröße sind es vor allem Befragte aus Firmen mit 500 bis 1.000 Mitarbeitern, die entsprechend gut Bescheid wissen – hier schätzen ihn rund 83 Prozent als groß oder sehr groß ein.

4.1.2 Wissensstand der Bürger und Politiker bezüglich der Risiken im Internet

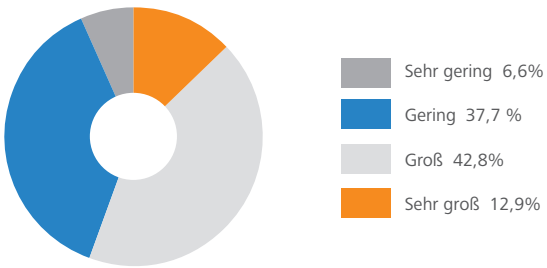
Fast 72 Prozent der Befragten meinen, dass das Wissen der Bürger über die Risiken im Internet – für ihre Grundrechte und für die Wirtschaft – generell zu gering sei. Es fehlen also Aufklärung und der gesellschaftliche Diskurs.

Die Politiker gelten insgesamt als besser informiert als die Bürger. Dies wirkt sich jedoch nicht positiv auf die Gesamtbewertung des politischen Handelns aus, wie die Einschätzungen zum Vertrauen und zur politischen Arbeit zeigen.

4.1.3 Potentielle Angriffe: Ausgeprägtes Bewusstsein für die Gefahren

Der Großteil der Umfrageteilnehmer ist sich der Gefahren eines Angriffs auf ihr Unternehmen beziehungsweise ihre Organisation bewusst. Mehr als die Hälfte (55,7 Prozent) schätzt die Gefahr eines Angriffs als groß bzw. sehr groß ein.

Für wie groß halten Sie die Gefahr, dass Ihr Unternehmen Opfer von Angriffen im IT-Bereich wird? Sei es durch Hacker, Viren, Trojaner, Wirtschaftsspionage o.ä.?



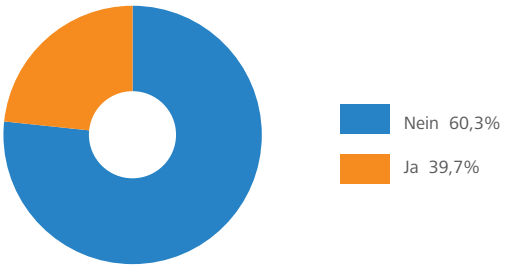
LANCOM Systems

Am sichersten fühlen sich noch Entscheider aus der öffentlichen Verwaltung bzw. aus Nicht-Regierungsorganisationen (NGOs). Von ihnen schätzen nur rund 43 Prozent die Gefahr, dass ihre Organisation Opfer von Angriffen im IT-Bereich wird, als sehr groß oder groß ein. Unter allen Befragten tun dies immerhin fast 56 Prozent, bei den Umfrageteilnehmern aus Industrie und Bau sogar 69,1 Prozent. Bezogen auf die Unternehmensgröße sind es vor allem Unternehmen mit 500 bis 1.000 Mitarbeitern, die in diesem Punkt alarmiert sind (72,1 Prozent). Diejenigen, die ihre IT-Kompetenz als sehr hoch einschätzen, sind sich der Gefahren wesentlich bewusster als Mitarbeiter mit geringerer IT-Kompetenz (73,9 Prozent).

4.1.4 Tatsächliche Angriffe: Unterschiedliche Wahrnehmung über erfolgte Angriffe oder „Aus Erfahrung wird man klug“

Die Frage, ob es bereits Angriffe auf das Unternehmen gab und ob diese den Umfrageteilnehmern bekannt sind, beantworteten fast 40 Prozent der Umfrageteilnehmer mit „Ja“. Über die geringsten eigenen Erkenntnisse über bereits erfolgte Angriffe verfügen die Entscheider aus der öffentlichen Verwaltung bzw. aus NGOs und aus der Dienstleistungsbranche.

Sind Ihnen Angriffe auf Ihr Unternehmen bekannt?



Unternehmen mit 500 bis 1.000 Mitarbeitern waren am häufigsten von einem Angriff betroffen (58,1 Prozent). Bei kleinen Unternehmen mit bis zu 50 Mitarbeitern waren es nur 24,5 Prozent.

Interessant ist, dass dem oberen Management mit gut 61 Prozent offenbar mehr Angriffe bekannt sind als der Geschäftsführung mit knapp 31 Prozent. Hier liegt die Vermutung nahe, dass es eine unterschiedliche Wahrnehmung hinsichtlich der Bedeutung eines Angriffs gibt. Möglicherweise ist die Bereitschaft, erfolgte Angriffe öffentlich zu kommunizieren, in der Geschäftsleitung auch weniger ausgeprägt. Es ist auch denkbar, dass die Geschäftsführung nicht über alle Angriffe informiert wird oder sich nur im absoluten Ernstfall dafür interessiert.

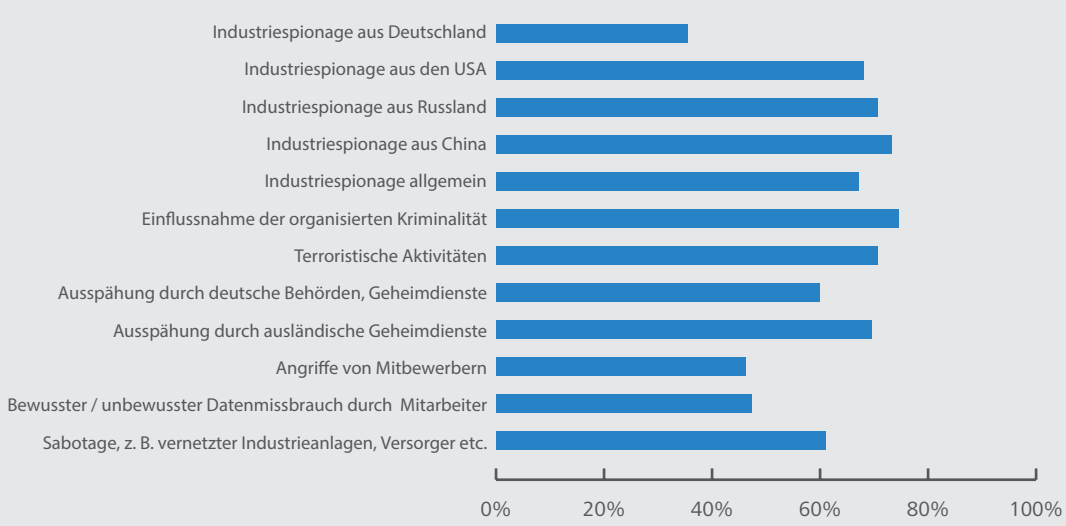
Mit zunehmendem Alter ist das Risikobewusstsein schwächer ausgeprägt. Ob Entscheider mit mehr „Lebenserfahrung“ abgeklärter mit Risiken umgehen oder den neuen Herausforderungen weniger sensibel gegenüberstehen, muss offen bleiben.

Die unmittelbare Erfahrung von Angriffen auf die IT und die IT-Kompetenz sind offenbar die entscheidenden Faktoren für das Risikobewusstsein. Würde intern stärker über IT-Sicherheitsvorfälle informiert, wäre auch das Risikobewusstsein ausgeprägter.

4.1.5 Angstszenarien: Organisierte Kriminalität, Industriespionage aus China und terroristische Aktivitäten

Die Teilnehmer wurden in der Untersuchung befragt, vor welchen Szenarien im Internet sie besonders viel Angst haben. Die Ergebnisse fielen deutlich aus: Fast 75 Prozent und damit drei von vier Befragten fürchten die Einflussnahme der organisierten Kriminalität stark oder sehr stark, gefolgt von Industriespionage aus China (73,3 Prozent) und terroristischen Aktivitäten (70,6 Prozent). Es folgen die Ausspähung durch ausländische Geheimdienste (69,6 Prozent) sowie Industriespionage aus den USA (68,1 Prozent). Industriespionage aus Deutschland wird von den Umfrageteilnehmern am wenigsten befürchtet (35,5 Prozent).

Ich habe Angst vor folgenden möglichen Szenarien im Internet
Antwort: viel / sehr viel



4.2 Vertrauensfragen

Ein zentrales Thema der Befragung war Vertrauen. Der durch die Snowden-Enthüllungen entstandene Vertrauensverlust war sicherlich der Ausgangspunkt für die Debatte um die Digitale Souveränität. Welchen Personen und Einrichtungen können wir heute vertrauen? Wie steht es um die Vertrauenswürdigkeit der Regierungen einzelner Länder? Wie weit können wir Internet-Konzernen vertrauen?

4.2.1 Personen und Einrichtungen in Deutschland: Die IT-Abteilung genießt am meisten Vertrauen, der BND am wenigsten

Die Antworten auf die Frage, welchen Einrichtungen/Personen die Teilnehmer vertrauen, fallen deutlich zugunsten der internen IT-Abteilung aus. Bei ihr gehen 72,8 Prozent der Befragten uneingeschränkt oder zumindest sehr davon aus, dass sie ihren Einfluss nicht gegen die Interessen der Bürger und Unternehmen in Deutschland einsetzt.

Es folgen mit deutlichem Abstand die externen IT-Partner oder Dienstleister mit 51,6 Prozent – ihnen vertraut jeder zweite Befragte uneingeschränkt oder sehr.

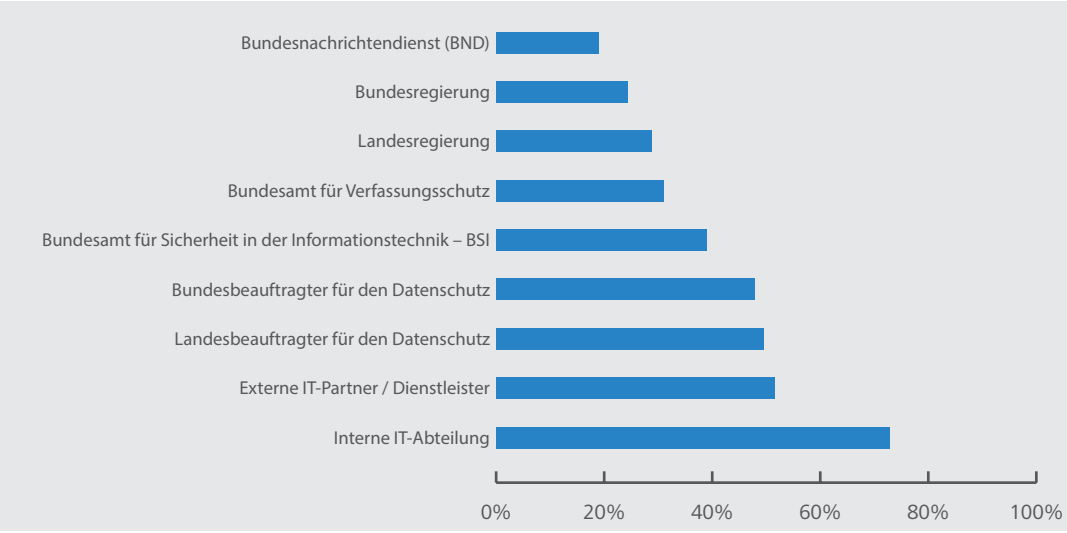
Eine ähnliche Bestätigung bei der Vertrauensfrage wie die IT-Partner – und zwar von fast jedem zweiten Befragten – erhalten die Landesbeauftragten für den Datenschutz und die Bundesbeauftragten für den Datenschutz.

Am schlechtesten schneiden in puncto Vertrauen der deutsche Geheimdienst, einige Behörden und die Regierung ab. Das Schlusslicht bei der Vertrauenswürdigkeit bildet der Bundesnachrichtendienst BND (19,7 Prozent) – ihm wird am wenigsten Vertrauen entgegengebracht. Das Image des BND hat durch die Enthüllungen und Negativschlagzeilen der letzten Wochen – Stichwort Geheimdienstaffäre – offensichtlich massiv gelitten.

Dem Bundesamt für Sicherheit in der Informationstechnik, BSI, bringen die Großunternehmen (ab 1.000 Mitarbeitern) noch das größte Vertrauen entgegen, allerdings vertraut nur jeder zweite Befragte (47,6 Prozent) ihm uneingeschränkt oder sehr. Dieses Ergebnis stimmt nachdenklich und spricht für eine gezielte Förderung von vertrauensbildenden Maßnahmen.

Der Bundesregierung vertraut nur knapp jeder vierte Befragte (24,3 Prozent) uneingeschränkt oder sehr. Auch hier ist das Vertrauen beschädigt. Das Verhalten der Regierung war in den letzten Wochen und Monaten sicher nicht vertrauensbildend, „Vernebelungen und Vertuschungen" wurden ihr vorgeworfen.

Welchen Einrichtungen und Personen vertrauen Sie, dass sie ihren Einfluss nicht gegen die Interessen der Bürger und Unternehmen in Deutschland einsetzen?
Antwort: uneingeschränkt / sehr



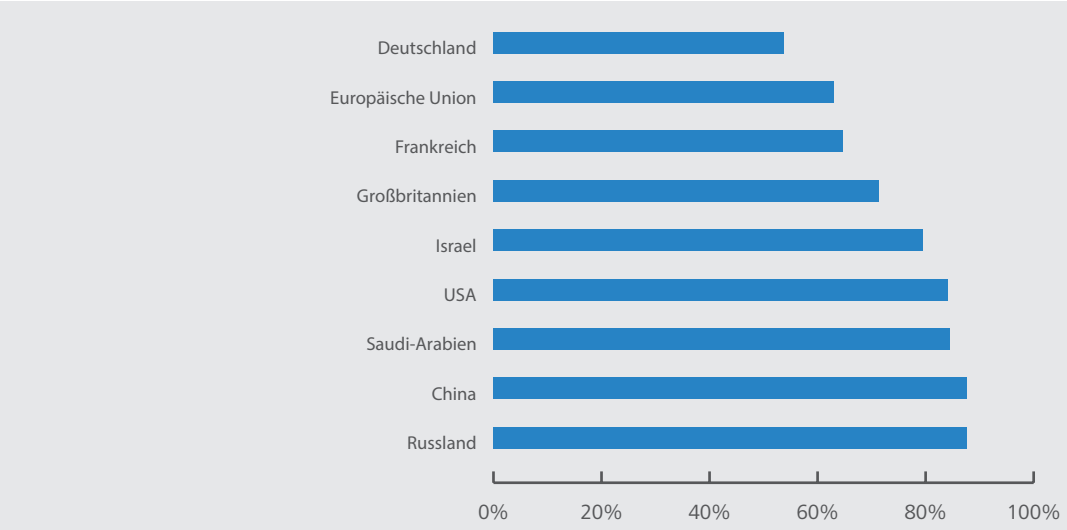
Fazit: Die Politik ist dringend gefordert, das Vertrauen in wichtige Institutionen wieder zu stärken.

4.2.2 Regierungen: China und Russland Schlusslicht bei der Vertrauensfrage

Die Umfrage ging auch der Frage nach, welchen Regierungen die Teilnehmer insofern vertrauen, dass diese ihren Einfluss nicht gegen die Interessen der Bürger und Unternehmen in Deutschland einsetzen.

Wenig oder kein Vertrauen wird in diesem Punkt den Regierungen Chinas (87,6 Prozent), Russlands (87,6 Prozent), Saudi-Arabiens (84,5 Prozent) und der USA (84,1 Prozent) attestiert. Auch das Vertrauen in die deutsche Regierung ist offensichtlich strapaziert worden: Das erklärt den relativ hohen Wert von 53,8 Prozent. Die Europäische Union schneidet in dieser Fragestellung jedoch mit 63 Prozent um einiges schlechter ab als Deutschland.

Welchen Regierungen vertrauen Sie, dass sie ihren Einfluss nicht gegen die Interessen der Bürger und Unternehmen in Deutschland einsetzen?
Antwort: wenig oder gar nicht

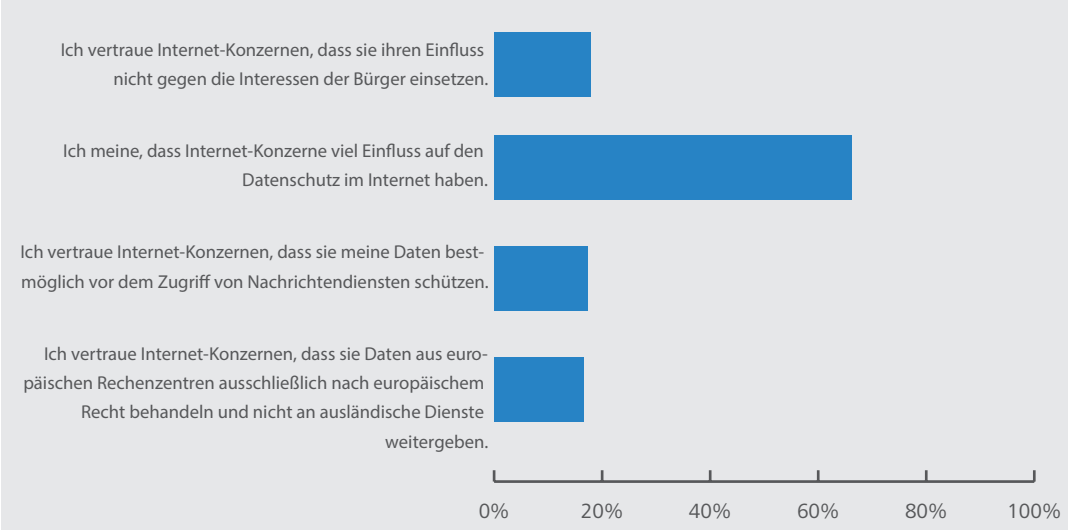


4.2.3 Internet-Konzerne: Geringes Vertrauen in Internet-Konzerne

Ausländische, oft monopolistische Internet-Unternehmen dominieren heute das Internet. Diese Tatsache bestätigen in der Umfrage 82,5 Prozent der Teilnehmer. In der Umfrage wurde ihr Einfluss auf den Datenschutz abgefragt. 66,2 Prozent sind der Meinung, dass Internet-Konzerne sehr viel bzw. viel Einfluss auf den Datenschutz im Internet haben.

In puncto Vertrauen schneiden Internet-Konzerne durchweg schlecht ab: Nur 17,8 Prozent der Umfrageteilnehmer sind der Meinung, dass sie ihren Einfluss nicht gegen die Interessen der Bürger einsetzen. Lediglich 17,3 Prozent vertrauen Internet-Konzernen insofern, als dass diese ihre Daten bestmöglich vor dem Zugriff von Nachrichtendiensten schützen. Und nur 16,5 Prozent sind der Meinung, dass sie Daten aus europäischen Rechenzentren ausschließlich nach europäischem Recht behandeln und nicht an ausländische Geheimdienste weitergeben.

Vertrauen in Internet-Konzerne
Antwort: stimme uneingeschränkt / sehr zu



Die Umfrage bestätigt die Annahme, dass das Vertrauen in Internet-Konzerne heute sehr gering ist. In dieses Bild passt auch die hohe Zahl an Befürwortern eines europäischen Gegengewichts zum Engagement der USA im Internet (84,4 Prozent), aber auch die hohe Übereinstimmung bei der Frage nach der Möglichkeit, Daten aus der EU nur in der EU zu speichern und zu verarbeiten (81,8 Prozent).

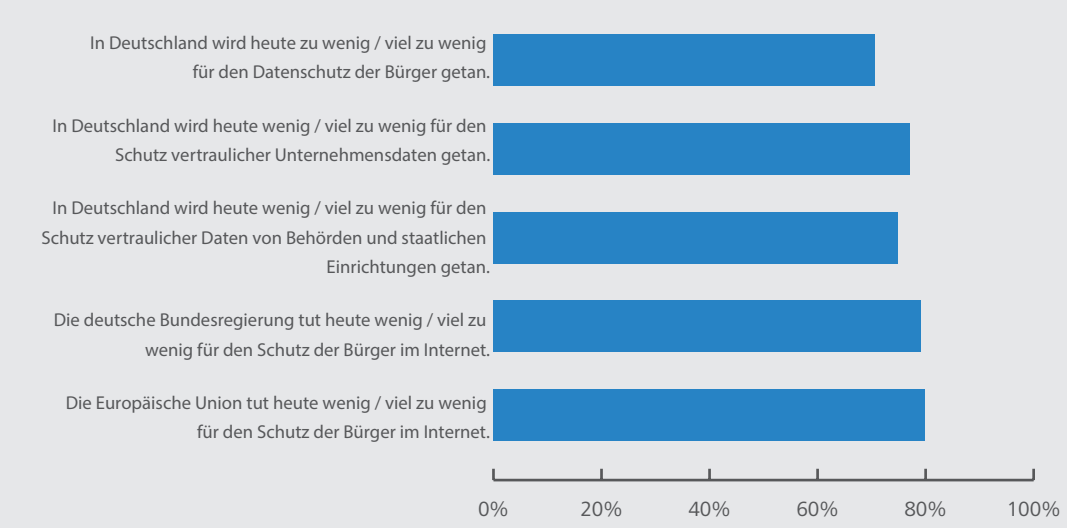
4.2.4 Vertrauliche Daten nicht ausreichend geschützt

Ein ernüchterndes Ergebnis gab es bei der Frage, was heute in Deutschland für den Datenschutz getan wird: 7 von 10 Befragten sind der Meinung, dass für den Datenschutz der Bürger zu wenig oder viel zu wenig getan wird (70,6 Prozent).

Ein schlechtes Zeugnis in puncto Datenschutz wird der Bundesregierung und der Europäischen Union ausgestellt, die mit jeweils knapp 80 Prozent Zustimmung wenig oder zu wenig für den Schutz der Bürger im Internet tun.

Drei von vier Befragten (77,1 Prozent) sind der Meinung, dass für den Schutz vertraulicher Unternehmensdaten zu wenig bzw. viel zu wenig getan wird. Ähnlich verhält sich das Bild bei der Frage nach dem Schutz sensibler Daten von Behörden und staatlichen Einrichtungen: 74,9 Prozent schätzen die Bemühungen als zu gering oder viel zu gering ein.

Was tun wir heute in Deutschland für den Datenschutz?
Antwort: wenig / viel zu wenig



Diese klaren Ergebnisse spiegeln die Ohnmacht beim Schutz sensibler Daten in Unternehmen, Behörden und den Kontrollorganen wider.

4.3 Digitale Souveränität

Digitale Souveränität war das Leitthema der Umfrage. Wie steht es heute um die Digitale Souveränität Deutschlands und Europas? Welche Maßnahmen können uns zu mehr Digitaler Souveränität verhelfen? Zu diesem zentralen Fragenblock lieferte die Umfrage eindeutige Ergebnisse.

4.3.1 Status Quo: Digitale Souveränität ist eine der dringendsten netzpolitischen Aufgaben

Im Kontext der Umfrage war besonders von Interesse, wie es heute um die Digitale Souveränität von Deutschland und Europa steht.

Edward Snowden hat uns deutlich vor Augen geführt, dass Deutschland und die EU digital nicht souverän sind – dieser Aussage stimmen 83,2 Prozent der Umfrageteilnehmer zu.

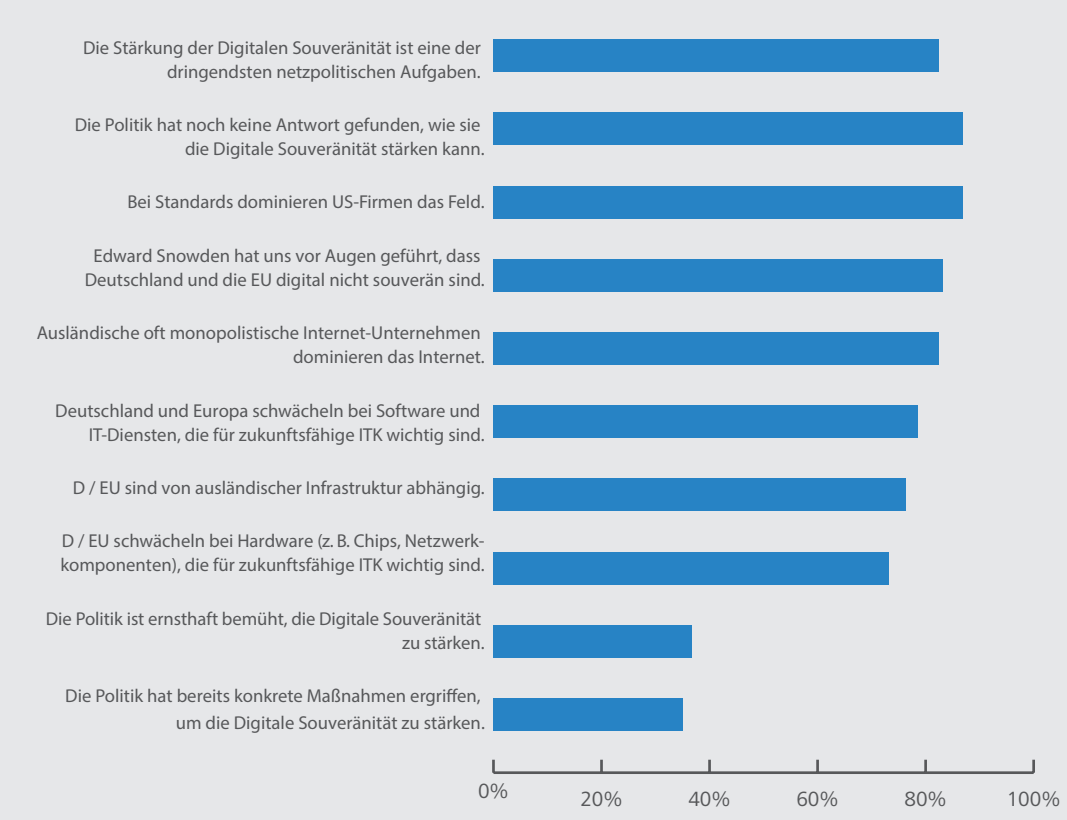
Deutschland und Europa sind von ausländischer Infrastruktur abhängig, meinen 76,4 Prozent der Befragten. In dieses Bild passt auch die hohe Zustimmung bei der Aussage, dass Deutschland und Europa bei Software und IT-Diensten, die für zukunftsfähige ITK wichtig sind, schwächeln (78,6 Prozent). Bei der Hardware sehen knapp 3 von 4 Befragten (73,2 Prozent) diese Schwäche der deutschen Industrie.

Eine der höchsten Zustimmungen erzielte die Aussage, dass bei den Standards US-Firmen das Feld dominieren (86,9 Prozent).

Ein schlechtes Zeugnis wird der Bundesregierung ausgestellt: Knapp 9 von 10 der Befragten sind der Meinung, dass die Politik noch keine Antwort gefunden hat, wie sie die Digitale Souveränität Deutschlands beziehungsweise Europas stärken kann. Diese Aussage erhielt mit 89,3 Prozent die höchste Zustimmung bei den Teilnehmern. Entsprechend wenig Zustimmung – von drei von zehn Befragten – gab es auf die Frage, ob die Politik ernsthaft bemüht sei, die Digitale Souveränität zu stärken (36,8 Prozent) und ob sie bereits konkrete Maßnahmen zur Erreichung dieses Ziels ergriffen habe (35 Prozent).

Das ist als klarer Appel an die Regierung zu verstehen: Hier besteht dringender Handlungsbedarf – die Stärkung der Digitalen Souveränität gehört zu den dringendsten netzpolitischen Aufgaben in Deutschland und Europa. Dieser Aussage stimmen so auch 82,5 Prozent der Befragten zu.

Wie steht es um die Digitale Souveränität Deutschlands und Europas?
Antwort: stimme überwiegend / sehr zu



4.3.2 Gefahren: Backdoors sind das Aus für die Digitale Souveränität

Backdoors, also geheime Zugangsmöglichkeiten in IT-Produkten, werden von 84,7 Prozent der Umfrageteilnehmer als Gefahr für die Digitale Souveränität angesehen.

Zu diesem Ergebnis passt auch die Maßnahme im Rahmen des IT-Sicherheitsgesetzes, dem BSI erstmals die Befugnis zu geben, IT-Produkte tiefgehend auf Schwachstellen und Backdoors zu überprüfen, notfalls mittels Reverse Engineering. So ist man erstmals in der Lage, zu beurteilen, ob ein Produkt die gewünschten Sicherheitseigenschaften besitzt und die Hersteller vertrauenswürdige Anbieter und Partner sind. Ein hoher Prozentsatz der Befragten erachtet in diesem Zusammenhang gezielte Sicherheitsüberprüfungen von ausländischen IT-Produkten als geeignet, die Digitale Souveränität zu stärken (81,5 Prozent).

Bei der Frage, ob das Transatlantische Freihandelsabkommen TTIP eine Gefahr für die Digitale Souveränität darstellt, war das Bild weniger eindeutig. Dieses noch relativ junge Thema ist offensichtlich noch nicht so stark in den Köpfen verankert.

4.3.3 Ein Blick in die Zukunft: Industrie 4.0 und Cloud Computing

Digitale Souveränität wird von einem Großteil der Befragten (80,8 Prozent) als Voraussetzung für eine erfolgreiche Digitalisierung von Produktionsprozessen – Stichwort Industrie 4.0 – angesehen.

Digitale Souveränität gilt bei 84,9 Prozent der Umfrageteilnehmer auch als wesentliche Voraussetzung für eine sichere Nutzung von Cloud-Diensten.

Wenn Deutschland bei diesen wichtigen Zukunftsbereichen eine führende Rolle einnehmen will, gilt es die Digitale Souveränität Europas und Deutschlands zu stärken.

4.3.4 Maßnahmen: Sicherheit und Vertrauenswürdigkeit schaffen

Neben dem Aspekt der Sicherheit ist es vor allem die Vertrauenswürdigkeit des Anbieters, auf die bei der Wahl von IT-Lösungen ein besonderes Augenmerk gelegt werden muss, meinen 84,7 Prozent der Befragten.

Doch was können sinnvolle Maßnahmen sein, die von staatlicher Seite ergriffen werden sollten, um Digitale Souveränität zu stärken?

Die Aufnahme von Vertrauenswürdigkeitskriterien bei der Vergabe von öffentlichen Aufträgen, gezielte Sicherheitsüberprüfungen ausländischer IT-Produkte oder auch die Prüfung der Vertrauenswürdigkeit von IT-Komponenten durch nationale oder europäische Stellen sind sinnvolle Möglichkeiten. Eine durchweg hohe Zustimmung – von rund acht von zehn Befragten – erhalten so auch diese Maßnahmen.

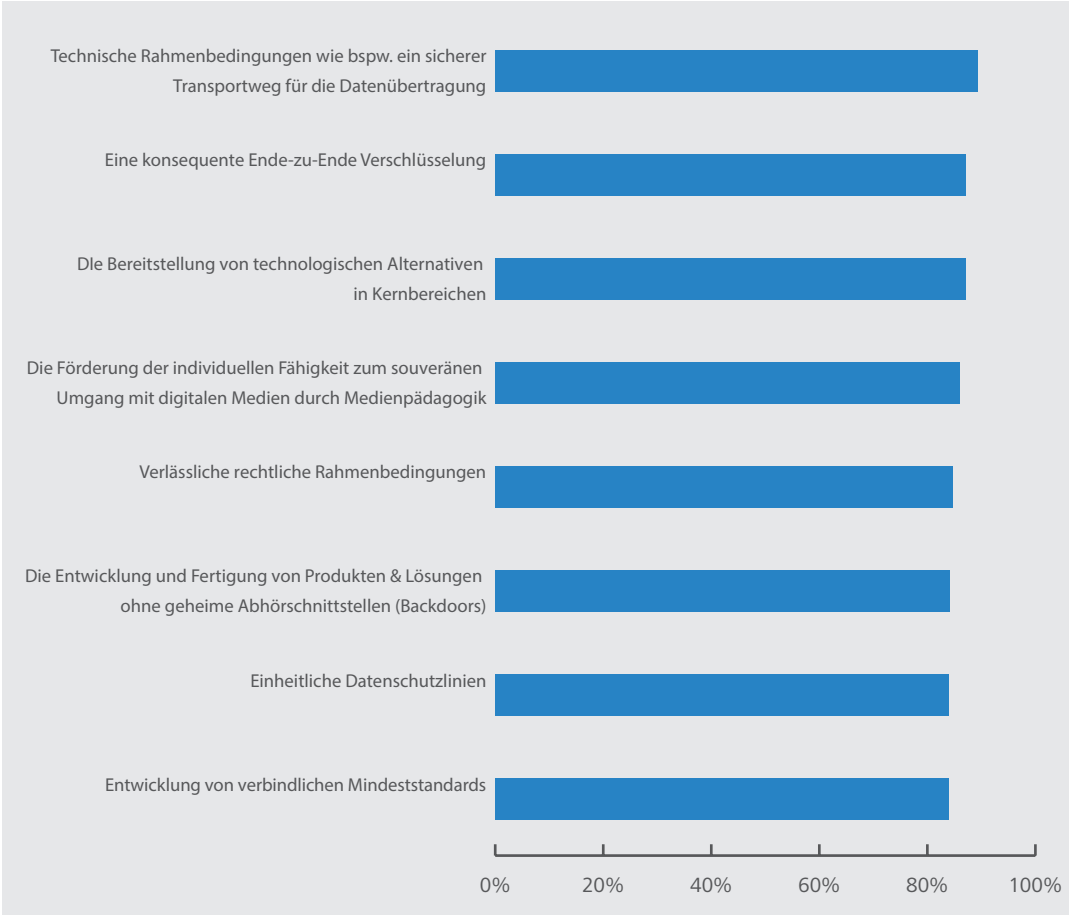
Technisch gesehen können ein sicherer Transportweg für die Datenübertragung (88,8 Prozent) und eine konsequente Ende-zu-Ende-Verschlüsselung (87,1 Prozent) ganz wesentlich zu mehr Digitaler Souveränität beitragen. Das meinen in der Umfrage fast neun von zehn Befragten.

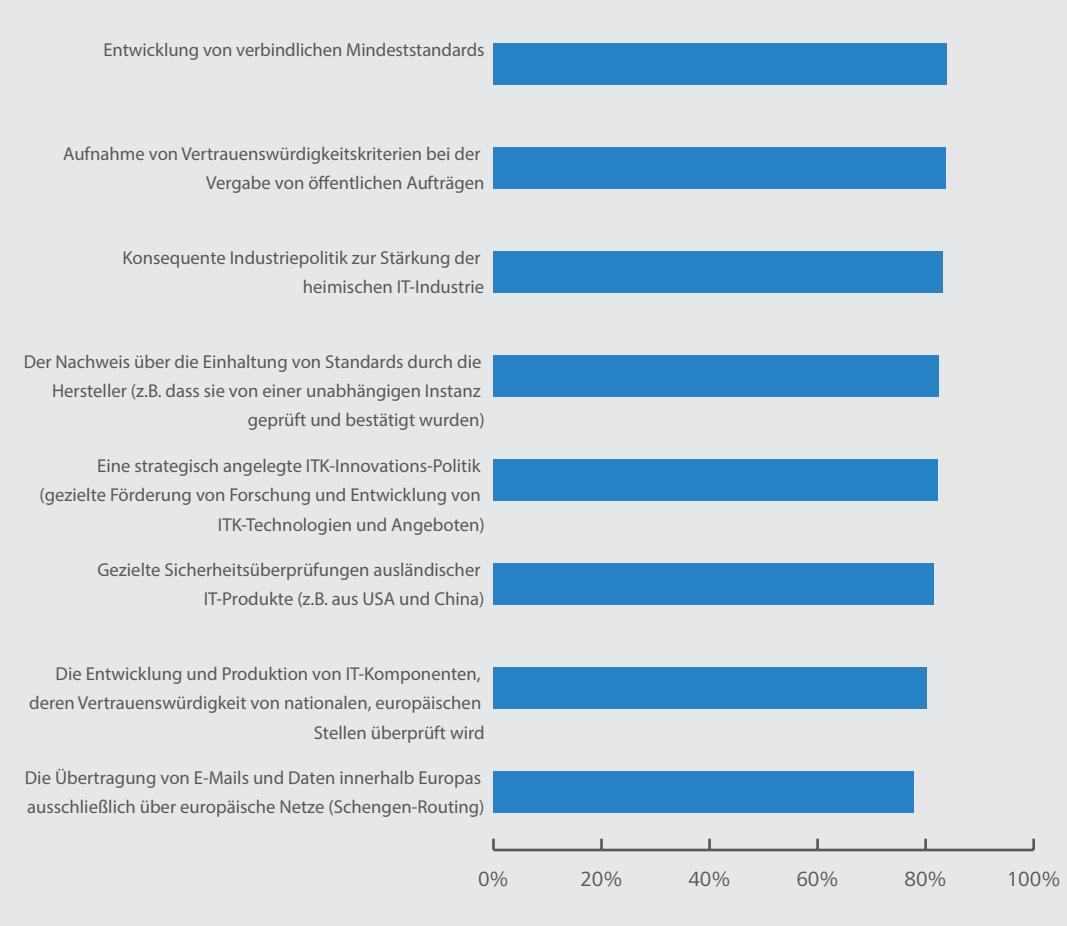
Generell ist die Politik gefordert, die Grundlagen für Digitale Souveränität zu schaffen: Mit verlässlichen rechtlichen Rahmenbedingungen (84,7 Prozent Zustimmung), einheitlichen Datenschutzrichtlinien (83,9 Prozent), verbindlichen Mindeststandards (83,9 Prozent), einer konsequenten Industriepolitik zur Stärkung der heimischen Industrie (83,2 Prozent) oder einer strategisch angelegten ITK-Innovationspolitik, d. h. der gezielten Förderung von Forschung und Entwicklung von ITK-Technologien und Angeboten (82,2 Prozent).

Im Ergebnis sollten – so auch der Wunsch von 87,1 Prozent der Befragten – mehr technologische Alternativen in Kernbereichen bereitgestellt werden. Und diese sollten ohne geheime Abhörschnittstellen entwickelt und gefertigt werden (84,2 Prozent).

Nicht zuletzt darf die Förderung der individuellen Fähigkeit zum souveränen Umgang mit digitalen Medien durch Medienpädagogik als eine der zentralen Forderungen in der Umfrage keinesfalls außer Acht gelassen werden – 85,9 Prozent der Umfrageteilnehmer favorisieren diese Maßnahme. Aufklärungs- und Erziehungsarbeit ist deshalb unbedingt erforderlich.

Welche Maßmahmen sind erforderlich, um die Digitale Souveränität (bezogen auf unser Land) zu erlangen? Antwort: stimme überwiegend / sehr zu





5. Fazit

Die Ergebnisse der Umfrage machen deutlich, dass es um die Digitale Souveränität Deutschlands und Europas nicht gut bestellt ist. Entscheider der deutschen Wirtschaft und Verwaltung wünschen sich (mehr) Digitale Souveränität und haben eine klare Vorstellung davon, wie diese gestärkt werden kann. Der Politik wird dabei ein schlechtes Zeugnis ausgestellt. Sie hat nach Ansicht der Umfrageteilnehmer noch keine Antwort darauf gefunden, wie sie die Digitale Souveränität stärken kann. Nach dem Eindruck der Befragten ist sie weder bemüht noch hat sie ernsthaft Maßnahmen ergriffen, die Digitale Souveränität Deutschlands zu sichern.

Generell spielen bei der Auswahl von IT-Produkten Vertrauen und Vertrauenswürdigkeit heute eine ganz wesentliche Rolle. Die Snowden-Enthüllungen haben uns nicht nur vor Augen geführt, dass Deutschland und die EU nicht digital souverän sind, sie waren auch Ausgangspunkt der Vertrauensdebatte. Deutschland ist heute stark von ausländischen IT-Angeboten abhängig, deren Vertrauenswürdigkeit mindestens in Teilen fraglich ist. Dazu kommt, dass für den Schutz vertraulicher Unternehmens- und Behördendaten viel zu wenig getan wird. Das sieht auch ein Großteil der Umfrageteilnehmer so und ist entsprechend besorgt. Datenschutz wird umso wichtiger.

Es geht also nicht nur um Sicherheit, es geht auch um Vertrauenswürdigkeit. Das bedeutet, dass man sich auf technische Komponenten verlassen kann und, noch wichtiger, dass man deren Herstellern vertrauen kann. Dazu müssen Unternehmen und Behörden jedoch in der Lage sein: Wie können sie erkennen, ob ausländische Hersteller auch vertrauenswürdige Partner und ihre Lösungen ebenso zuverlässig sind? Die Beurteilungsfähigkeit spielt eine wesentliche Rolle für die digitale Selbstbestimmung.

Hier muss die Politik ihren Beitrag leisten. Erste sinnvolle Vorstöße gibt es bereits: Das BSI wird im Rahmen des IT-Sicherheitsgesetzes erstmals die Befugnis haben, IT-Produkte tiefgehend auf Schwachstellen und Backdoors zu überprüfen. Eine wichtige Maßnahme, um beurteilen zu können, ob ein Produkt die gewünschten Sicherheitseigenschaften besitzt und dessen Hersteller ein vertrauenswürdiger Anbieter ist. Gezielte Sicherheitsüberprüfungen von ausländischen IT-Produkten werden von einem Großteil der Teilnehmer als wesentliche Maßnahme für mehr Digitale Souveränität erachtet. Die Aufnahme von Vertrauenswürdigkeitskriterien bei der Vergabe von öffentlichen Aufträgen zielt in eine ähnliche Richtung und wird in der Umfrage stark befürwortet. Auch das von der Politik abgelehnte Schengen-Routing erfährt als möglicher Baustein eine hohe Zustimmung. Solche Maßnahmen können auch vertrauensbildende Schritte der Politik in eigener Sache sein –- das Vertrauen in die Bundesregierung hat offensichtlich gelitten. Dem BND wird in der Umfrage von allen Einrichtungen das geringste Vertrauen bescheinigt.

Aber es geht auch um Handlungs- und Entscheidungsfreiheit. Angesichts der dominanten Rolle von ausländischen Anbietern bei Internet-Technologien, vor allem der großen US-Konzerne, wird diese Freiheit immer wichtiger. US-Firmen dominieren vor allem bei den Standards das Feld. Der „alte Kontinent“ schwächelt bei Soft- und Hardware-Komponenten, die für zukunftsfähige IT-Lösungen wesentlich sind. In dieser Beobachtung stimmen die meisten Teilnehmer der Umfrage überein. Es müssen also Alternativen bereit gestellt werden.

Generell ist die Politik gefordert, die Rahmenbedingungen so zu gestalten, dass die hiesige IT-Industrie gestärkt wird: Mit verlässlichen rechtlichen Rahmenbedingungen, einheitlichen Datenschutzrichtlinien, verbindlichen Mindeststandards, einer konsequenten Industriepolitik oder einer strategisch angelegten ITK-Innovationspolitik.

Nur so wird Deutschland und Europa bei wichtigen Zukunftsfeldern – vernetzte Produktion, Industrie 4.0, Internet der Dinge oder Cloud – eine führende Rolle einnehmen können.

Kurz: Digitale Souveränität ist einer der dringendsten netzpolitischen Aufgaben.

Über LANCOM Systems

Die LANCOM Systems GmbH ist führender deutscher Hersteller zuverlässiger und innovativer Netzwerklösungen für Geschäftskunden. Mit seinen beiden Geschäftsbereichen VPN-Standortvernetzung und Wireless LAN (drahtlose Netze) bietet LANCOM professionellen Anwendern sichere, flexible Infrastrukturlösungen für alle lokalen und standortübergreifenden Netze. Das gesamte Kernportfolio wird in Deutschland entwickelt und gefertigt. Zudem bietet LANCOM BSI-zertifizierte VPN-Lösungen zur Absicherung besonders sensibler Netze und kritischer Infrastrukturen (KRITIS) gegen Cyber-Angriffe. LANCOM Systems hat seinen Hauptsitz in Würselen bei Aachen und weitere Standorte europaweit. Zu den Kunden zählen kleine und mittelständische Unternehmen, Behörden, Institutionen und Großkonzerne aus Deutschland, Europa und zunehmend auch dem außereuropäischen Ausland. Das Unternehmen ist Partner in der vom BSI initiierten Allianz für Cyber-Sicherheit.

Kontakt

LANCOM Systems GmbH
Pamela Krosta-Hartl
Director Corporate Communications & Affairs
Tel: +49 (0) 2405 / 49936-331

Eckhart Traber
Pressesprecher
Tel: +49 (0)89 / 6656178-67
E-Mail: presse@lancom.de
Web: www.lancom-systems.de