VOICE - Bundesverband der IT-Anwender e.V.

FAIRE MARKTBEDINGUNGEN
BÜROKRATIEABBAU
DIGITALE SOUVERÄNITÄT

VOICE
Bundesverband der
IT-Anwender e.V.

Positionen zur Bundestagswahl
'21

12 Forderungen zur Bundestagswahl

VOICE e.V.
Marktbedingungen für IT- und Digital-Anwenderunternehmen verbessern

VOICE-Positionen zur Bundestagswahl: Marktbedingungen für IT- und Digital-Anwenderunternehmen verbessern

VOICE – Bundesverband der IT-Anwender e.V. hat gemeinsam mit seinen 400 Mitgliedern und ihren 2600 Unternehmen 12 Positionen formuliert, die die wichtigsten Anforderungen der Anwenderunternehmen an die Politik adressieren. Dabei geht es einerseits um verbesserte Marktbedingungen also mehr Produktvielfalt und Wettbewerb unter den Anbietern, weniger Lasten und Risiken sowie mehr Rechte für die Anwenderseite. Das gilt zum Beispiel für mehr Herstellerverantwortung für die Qualität ihrer Produkte, mehr Mitsprache bei Standards oder einfachere Softwareverträge.

Zum anderen verlangt VOICE Nachbesserungen für das AÜG, die DSGVO und das IT-Sicherheitsgesetz, um die Gesetze handhabbarer und aufwandsärmer zu gestalten und so den Interessen der vielen Tausend Anwenderunternehmen in Deutschland besser gerecht zu werden.

Kurzübersicht der VOICE-Forderungen:

Verbesserte Marktbedingungen, stärkere digitale Souveränität

1 Offene Standards für mehr Wettbewerb

Mit der Durchsetzung offener Standards den Wettbewerb stärken.
- Nutzung offener Standards insbesondere für Softwareschnittstellen und Datenaustauschformate erzwingen
- Pflege und Weiterentwicklung der offenen Standards durch paritätisch von Anwendern und Anbietern besetzte Gremien

2 Mehr Innovation für mehr digitale Souveränität

Gezielte Förderung digitaler Innovationen und Know-how-Aufbau für alle Wertschöpfungselemente der Digitalisierung.
- Einsatz europäischer IT-Komponenten gezielt fördern
- Förderung des Produkt-Reifeprozesses durch konstruktives Feedback von Anwendern
- Praxisorientierte Innovationspartnerschaften initiieren

3 GAIA-X muss europäisch bleiben

Digitale Souveränität: Bei GAIA-X in der Startphase ausschließlich Anbieter aus Europa einbeziehen.
- Vorzugsweise mittelständische europäische Anbieter in Führungsrollen bringen
- Schnelle Umsetzung durch Fokus auf Kernfunktionalitäten

4 Anbieter haften für ihre Produkte

Produkthaftung für Softwareprodukte auch im B2B-Geschäft.
- Anbieter haften für direkte und indirekte Schäden durch Produktmängel
- Qualitätsmängel bei IT-Security-Produkten als besonders schwerwiegend bewerten

5 Produktsicherheit wird Pflicht für Anbieter

IT-Security: Software und Cloudservices müssen sicher gestaltet sein.

- Strafbewehrte Verpflichtung von Software- und Internetanbietern zu hoher Produktqualität (Stand der Technik)
- Fehlerbeseitigung muss schnell erfolgen
- Aufwand für Anwenderseite minimal halten

6 Einfachere Softwareverträge

Regulierung der Software-Nutzungsverträge und Lizenzvereinbarungen.

- Verträge vereinfachen
- Einseitige Änderungsmöglichkeiten einschränken
- Unrechtmäßige Nutzung technisch ausschließen, um Audits überflüssig zu machen

7 Hilfen für Start-ups

Hands-on-Förderung verbessern.

- Ausbildung unternehmerischer Fähigkeiten gezielt unterstützen
- Coaching junger Unternehmen fördern
- Entrepreneurship-Lehrgänge flächendeckend in Hochschulen anbieten

8 Datenverkehr im Internet konsequent schützen

Sicherheit im Internet erhöhen, „Autokennzeichen und Leitplanken für das Web".

- Breite deutsche/europäische Initiative der Politik für mehr Sicherheit im Datenverkehr
- Aktiv gestaltende Rolle der Regierung bei der Weiterentwicklung des Internets zu einer sicheren Basisinfrastruktur der Wirtschaft
- Nachweisplichten für Kommunikationsteilnehmer (Server, Router und Netzknoten)
- Nachweispflichten für Domain-Halter (Vorbild: Handelsrecht)

9 Flexible Arbeitsformen erlauben

Arbeitnehmerüberlassungsgesetz (AÜG): Höchstüberlassungsdauer für Leiharbeitnehmer in der IT-Branche abschaffen.

- Leiharbeitnehmer mehr als 18 Monate für einen Kunden
- Rechtliche Voraussetzungen für weitere flexible Arbeitsformen schaffen

10 DSGVO Schutz vor Datenmissbrauch

DSGVO Schutz vor Datenmissbrauch wirksamer gestalten und Digitalisierung erleichtern.

- Datenverarbeitung bei konsequenter Einhaltung von Sicherheitsmaßnahmen erlauben und fördern
- Analysen als dedizierte Dienstleistung für den Datenlieferanten erleichtern
- De-Anonymisierung konsequent verbieten

Weniger Bürokratie, präzisere Regeln

11 IT-Sicherheitsgesetz 2.0 praxistauglich machen

Unterstützung statt Sanktionierung

- Anwenderunternehmen in Ausführungspraxis einbeziehen
- Meldepflichten handhabbar machen
- Klare und langfristig geltende Definition der betroffenen Unternehmen festlegen

12 BetrVG: Mitbestimmungsprozess bei IT-Systemen vereinfachen

- Präzisierung des § 87 Betriebsverfassungsgesetz, um Rechtsunsicherheit beim Einsatz von IT-Systemen zu beseitigen.
- Mitbestimmung auf Funktionen mit Gestaltungsspielraum beschränken.
- Festlegen, welche Systemfunktionen und Auswertungsmethoden erlaubt sind.
- Vorwegnahme von Updates erlauben.

Die 12 VOICE-Forderungen im Detail

Verbesserte Marktbedingungen, stärkere digitale Souveränität

1

IT-Märkte: Mit offenen Standards den Wettbewerb stärken.

VOICE fordert die Förderung offener Standards für flexible Software-Schnittstellen und Datenaustauschformate zwischen den Plattformen großer Softwareanbieter und anderer Softwarelösungen im Interesse der Anwender.

Eine der wesentlichen Ursachen für das derzeitige Marktversagen im Bereich der großen Plattformanbieter liegt in der Verwendung von proprietären, ausschließlich von einzelnen Herstellern kontrollierten Software-Schnittstellen (Application Programming Interfaces=APIs), an die auf der Nutzerseite hohe Investitionen vor allem in die Systemkonfiguration, ergänzende Teilfunktionen und die Prozessgestaltung gebunden sind.

Sogenannte Offene Standards für Software-Schnittstellen werden von Nutzern und Herstellern gemeinsam kontrolliert und sind ohne Vorbedingungen auch durch neue Marktteilnehmer nutzbar. Aufgrund ihrer hohen Langzeitstabilität und der angestrebten Aufwärts- bzw. Abwärtskompatibilität senken sie die Eintrittsrisiken für neue Wettbewerber und verringern die Abhängigkeit der Kunden von einzelnen Anbietern. Offene Standards stellen deshalb einen der wesentlichen Garanten für funktionierende Märkte dar.[1]

Um die für die Erarbeitung und Pflege offener Standards benötigten Gremien aufzubauen bzw. zu stärken, fordert VOICE ein Eingreifen der Bundesregierung bzw. des Gesetzgebers, mindestens in der Initialphase. Nur so kann bei den herrschenden Marktbedingungen der überbordende Einfluss einzelner Anbieter kompensiert werden.

Des Weiteren muss die öffentliche Hand als Vorreiter die Verwendung offener Standards fördern, indem diese in Ausschreibungen zur Bedingung gemacht werden.[2] Ein flächendeckender und konsequenter Einsatz ermöglicht kontinuierliche, intensive Rückmeldungen an die Standardisierungsgremien, um die fortwährende Optimierung zu ermöglichen.

Offene Standards für Software—Schnittstellen in diesem Sinne müssen folgende Eigenschaften aufweisen:

- Sie ermöglichen eine unwiderrufliche, freie Nutzung ohne Vorbedingungen. Ihre Definition ist folglich eine vorkommerzielle, gemeinnützige Aktivität der interessierten Marktteilnehmer.
- Sie sind vollständig und verständlich dokumentiert und für alle Marktteilnehmer gleichermaßen frei zugänglich.
- Die Weiterentwicklung folgt einem transparenten und öffentlich nachvollziehbaren Entscheidungsprozess, der insbesondere das Feedback der verschiedenen Nutzergruppen einbezieht und der von Fachexperten überprüft werden kann.
- Im Weiterentwicklungs- und Pflegeprozess liegt ein Schwerpunkt auf der Gewährleistung maximaler Kompatibilität neuer Versionen mit den im Markt befindlichen Anwendungen, sodass für alle Marktteilnehmer eine hohe Investitionssicherheit entsteht.
- Softwaremodule, die von den offenen Standards Gebrauch machen, können dabei Open-Source oder proprietär sein, solange sie an allen Schnittstellen den offenen Standards folgen.
- In die Standardisierung ist dabei insbesondere auch die Schnittstelle zwischen dem menschlichen Anwender und den Softwaresystemen mit einzubeziehen.

Zu den bevorzugt zu standardisierenden Schnittstellen gehören insbesondere Dateiformate zur Übertragung von Datenobjekten zwischen Softwaremodulen (.vcf, .ics, .odf, .step etc.).[3] Wo es gelungen ist, solche Formate zu stabilen Standards zu entwickeln, hat dies sehr positiv zur Produktvielfalt und zum Wettbewerb beigetragen.

[1] In einigen Marktsegmenten werden solche offenen Standards bereits sehr erfolgreich eingesetzt (Hardware-Interface in Server-Systemen, USB-Peripheriegeräte etc.). In diesen Segmenten ist der resultierende Wettbewerb hoch und die Qualität folglich erfreulich hoch.

[2] Die britische Regierung hat die Verwendung offener Standards bereits 2018 definiert: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

[3] Dateiformate als offene Standards gibt es seit vielen Jahren. Ihre strikte Anwendung in kommerziellen Softwareprodukten wurde aber bisher nicht eingefordert. Öffentliche Auftraggeber müssen dies jetzt erzwingen, da die Umgehung insbesondere durch die Marktführer einer der wichtigsten Gründe für die starke ungewollte Bindung der Bestandskunden an diese Marktführer darstellt. Formate, die bereits in paritätisch besetzten Konsortien weiterentwickelt werden (.vcf = RFC 6350 und .ics = RFC 5545) leisten bereits einen sehr guten Beitrag zur Kompatibilität zwischen Softwaremodulen verschiedener Hersteller und tragen somit sehr viel zu einem funktionierenden Wettbewerb bei.

2

Digitale Souveränität: gezielte Förderung digitaler Innovationen und Know-how-Aufbau für alle Wertschöpfungselemente der Digitalisierung.

VOICE fordert die gezielte Förderung des Einsatzes europäischer IT-Komponenten zur Erhöhung der Unabhängigkeit und zur Belebung und Diversifizierung des Wettbewerbs in den Schlüsseltechnologien der Digitalisierung.

Digitale Infrastrukturen benötigen eine große Anzahl missionskritischer Schlüsseltechnologien, von denen derzeit nur ein kleiner Teil durch europäische Anbieter auf Augenhöhe mit ihren asiatischen und US-amerikanischen Wettbewerbern erbracht werden kann. Dies führt –zusätzlich zu den ohnehin vorhandenen negativen Effekten der Oligopole- zu außenpolitischen Abhängigkeiten und somit zu zusätzlichen Risiken für die Anwenderunternehmen. Zudem schränkt die Abhängigkeit die diplomatische Handlungsfähigkeit der EU gegenüber den anderen Wirtschaftsmächten massiv ein.

Die in den vergangenen Jahren verfolgte Förderpolitik mit Fokus auf Forschung und Innovationen reicht dabei nicht aus. Trotz exzellenter Spitzenforschung und eines hohen Innovationsgrades ist die Etablierung von Anbietern mit nennenswertem Marktanteil bislang nur in Ausnahmefällen gelungen. Was fehlt ist ein flächendeckender praktischer Einsatz der neuen IT-Produkten als bewusste Unterstützung des Reifeprozesses. Dabei kommt den Anwenderunternehmen auch die Aufgabe einer konstruktiven Rückmeldung für Optimierungen zu.

3

Digitale Souveränität: Bei GAIA-X in der Startphase ausschließlich Anbieter aus Europa einbeziehen.

VOICE fordert, das Projekt für eine eigenständige europäische Daten-Infrastruktur, GAIA-X, in den kommenden ersten Jahren vorzugsweise für mittelständische europäische Anbieter und Anwender zu öffnen.

Das Projekt GAIA-X hat zum Ziel, den Wettbewerb im Markt der Cloud-Plattformanbieter auch für mittelständische europäische Anbieter zu öffnen. Ziel ist es dabei, die bestehende Dominanz einzelner großer Plattformen mittels eines auf offenen Standards basierenden Software-Stacks (dem sog. Sovereign Cloud Stack) zu neutralisieren. Es ist klar, dass dies nicht im Geschäftsinteresse der hierdurch beschränkten Großanbieter sein kann. Bei einer Teilnahme dieser Anbieter, muss ferner von einem krassen Ungleichgewicht bzgl. der Ressourcen und des initialen Know-hows ausgegangen werden, was einer gedeihlichen Zusammenarbeit zwangsläufig entgegensteht. Herausforderungen im Aufbau des Standards sind keinesfalls auf der technischen, viel mehr aber auf der organisationspsychologischen Seite zu erwarten. Der Erfolg hängt letztlich von einem ausgeglichenen Kräfteverhältnis unter den Partnern ab.

VOICE fordert deshalb, diese Anbieter nicht an dem Konsortium zu beteiligen, sondern vorzugsweise mittelständische, europäische Anbieter in eine Führungsrolle zu bringen.
Dabei muss der Fokus auf die wenigen tatsächlich benötigten Kernfunktionalitäten gelegt werden, anstatt durch eine zu große Servicepalette Tempo zu verlieren.

Eine Mitarbeit der großen Anbieter ist dann anzustreben, wenn die erarbeiteten Standards im Markt etabliert und deren Einsatz insbesondere auf Seiten der Beschaffer als mandatorisch definiert ist.

4

Weitgehende Produkthaftung für Softwareprodukte auch im B2B-Geschäft.

VOICE fordert die konsequente Durchsetzung einer Haftung der Softwarehersteller für direkte und indirekte Schäden bei Anwenderunternehmen, die durch Qualitätsmängel entstehen.

Softwareprodukte haben für die Geschäftstätigkeit von Unternehmen und die staatlichen Verwaltungsprozesse eine überragende Bedeutung erlangt. Ihre Qualität bestimmt sowohl den Betriebsaufwand als auch die Sicherheitsrisiken. Dabei kann ein in der Entwicklung eingespartes Personenjahr leicht das zehnfache an Aufwand auf Seiten der Betreiber hervorrufen.[4] Anders als in anderen Industrien (Automobilbau, Anlagenbau) gibt es bisher jedoch keinen monetären Anreiz für Softwareanbieter, die Qualität ihrer Produkte auf einem hohen Niveau zu halten.

Die VOICE Mitglieder sehen die zusätzlichen Investitionen in die Entwicklung mit den folglich höheren Lizenzkosten als volkswirtschaftlich sinnvoll und als deshalb geboten an. Der finanzielle Anreiz für Softwarehersteller, in die Qualität ihrer Produkte zu investieren, muss durch entsprechende Vertragsstrafen und Schadensersatzansprüche geschaffen werden. Dabei sind insbesondere Sicherheitslücken in Produkten mit expliziten Sicherheitsaufgaben (Firewalls, Intrusion

4 Die heute als selbstverständlich hingenommenen, komplexen Prozeduren beim Update von Unternehmenssoftware machen in den Anwenderunternehmen den Einsatz hoch spezialisierter Fachkräfte sowie Betriebsunterbrechungen notwendig, obwohl bei entsprechenden Investitionen in die Produktentwicklung sowohl die Anzahl der Updates als auch der jeweils erforderliche Aufwand drastisch gesenkt werden könnte. Dass dies möglich ist, beweisen Produkte von kleinen Marktteilnehmern bzw. die Updateverfahren im Consumerbereich, bei denen Expertenwissen auf Kundenseite per se ausgeschlossen ist.

Detection / Prevention, Virenschutz) als besonders schwerwiegend zu bewerten und entsprechend zu ahnden. Die relevanten Gesetze und insbesondere die Rechtsprechung muss eine vereinfachte Durchsetzung der Ansprüche ermöglichen.

5

IT-Security: Software-Anbieter und Internetprovider müssen den Stand der Technik bzgl. minimaler Häufigkeit, Schnelligkeit und Handhabbarkeit von Sicherheitslücken erfüllen.

VOICE fordert die strafbewehrte Verpflichtung der Softwareanbieter und der Internetprovider zu angemessenen Maßnahmen zur Vermeidung von Fehlfunktionen bzw. zur zügigen, aufwands- und störungsfreien Beseitigung im Fehlerfall.

Die derzeitigen gesetzlichen Vorgaben zur Cybersicherheit beziehen sich nahezu ausschließlich auf die Verantwortlichkeiten der Anwenderunternehmen. Sie unterliegen Sorgfalts- und Meldepflichten (IT-Sicherheitsgesetz), tragen Verantwortung dafür, dass die von ihnen eingesetzte Technologie auf dem Stand der Technik befindet (z.B. Solvency 2) und selbstverständlich dafür, dass nachträgliche Fehlerbeseitigungen und die Schließung von Sicherheitslücken (Patches) zeitnah in die laufende IT-Umgebung eingespielt werden. Gleiches gilt im Bereich des Datenschutzes und der Internetsicherheit.

Um das bestehende Ungleichgewicht zu beseitigen, fordert VOICE die Verpflichtung der Software- und Serviceanbieter sowie der Internetprovider zu konkreten Maßnahmen zur Vermeidung bzw. zur zügigen Beseitigung von Sicherheitslücken. Der Gesetzgeber muss sie dazu verpflichten:

- den Stand der Technik bei der Produkt- und Servicequalität zu gewährleisten.
- bei auftretenden Sicherheitsmängeln diese binnen einer festgelegten zeitlichen Frist zu beheben und für das Ausbringen der entstehenden Patches einfache und betriebssichere Verfahren zur Verfügung zu stellen.
- die bekannten und erprobten Schutzmechanismen (z.B. DNSSEC) verpflichtend einzusetzen.

6

Regulierung der Software-Nutzungsverträge und Lizenzvereinbarungen.

VOICE fordert die Vereinfachung der Lizenzverträge sowie die Einschränkung von einseitigen Änderungsmöglichkeiten bzw. erweiterte Bindungs- und Ankündigungsfristen. Außerdem fordert VOICE von den Anbietern die unrechtmäßige Nutzung von lizenzierter Software sicher auszuschließen.

Die Lizensierung von Software und das Management von Software-Nutzungsverträgen nimmt im IT-Betrieb in Unternehmen und Verwaltung inzwischen einen signifikanten Anteil der Ressourcen in Anspruch. Dies ist auf zahlreiche einseitige Änderungen der Bedingungen und auf Vertragsklauseln mit zweifelhafter Rechtsgültigkeit zurückzuführen, die in den Anwenderunternehmen zu Unsicherheit und Managementaufwand führen.[5]

Aus Sicht der Anwenderunternehmen sind große Teile dieser Aufwände verzichtbar, wenn die zulässigen Vertragskonstruktionen gesetzlich detailliert geregelt würden. Dass dies bislang nicht durch den Wettbewerbsdruck selbst geschieht, ist auf das oben erläuterte Marktversagen zurückzuführen. Um dennoch einen rechtssicheren und vor allem aufwandsarmen IT-Betrieb zu ermöglichen, muss der Gesetzgeber entsprechende Vorgaben zu erlaubten Vertragsmodellen machen. Dabei sind insbesondere Vertragsänderungen zur Einschränkung der Nutzung und Veräußerung zu regeln bzw. die entsprechenden Klauseln explizit für rechtens/ nicht rechtens zu erklären sowie die erlaubten Änderungen im prinzipiellen Lizenzmodell (CPU-basiert, Concurrent User, Named User etc.) auf ein faires Maß zu beschränken.

Der Aufwand für das Lizenzmanagement lässt sich vor allem dadurch verringern, dass die Software selbst auf technischem Wege einen Missbrauch ausschließt (z.B. durch Lizenzschlüssel bzw. Token). Sofern eine Software nicht durch unzulässige Manipulation (sog. Crack) verändert wird, darf eine missbräuchliche Nutzung nicht möglich sein.

Zur Vereinfachung des Softwaremanagements muss die Vorinstallation der vollständigen Software (z.B. auf Arbeitsplatzrechnern) erlaubt sein, ohne dass dies im gleichen Zuge Lizenzkosten nach sich zieht. Erst die Installation des Lizenzschlüssels führt zur Inanspruchnahme der Softwarefunktion und somit zur Zahlungspflicht.

Sowohl auf Seiten der Anwenderunternehmen als auch bei den Herstellern von Softwareprodukten ist ein kontinuierlicher Cash-Flow wirtschaftlich vorteilhaft. Lizenzmodelle mit zeit- oder intensitätsbasierter Subskription („pay as you go") sind deshalb gegenüber Kaufoptionen zu bevorzugen. Sie schließen außerdem Konflikte über die Veräußerung von Kauflizenzen von vornherein aus. Entsprechend sind solche Abonnement-Verträge in den gesetzlichen Regelungen zu begünstigen.

[5] CISPE, ein europäischer Verband von Cloud-Anbietern (unter den Mitliedern ist unter anderem aws) hat gemeinsam mit dem französischen Anwenderverband und VOICE-Partnerverband CIGREF 10 Regeln für faire Software-Lizenzen für Cloud-Nutzer veröffentlicht. https://www.fairsoftware.cloud/principles/

7

Start-ups: Hands-on-Förderung verbessern.

VOICE fordert, digitale Start-ups intensiver und direkter zu fördern. Um gezielt Innovationen in Technologie und bei digitalen Geschäftsmodellen zu fördern, muss die deutsche und europäische Administration Mechanismen zur Förderung digitaler Start-ups entwickeln, die über steuerliche Anreize und bürokratische Vereinfachungen für Investoren und Gründer hinausgehen.

Insgesamt stagniert die Zahl der Start-Ups in Deutschland. Im Jahr 2020 waren es laut Förderbank KfW rund 70000 – nicht mehr als im Jahr 2018. Und das trotz der Tatsache, dass die Bundesregierung in den vergangenen Jahren das Gründen entbürokratisiert hat und verschiedene finanzielle Anreize für Investoren entwickelt hat (zum Beispiel Abschreibungsmöglichkeiten).

Zwar spielt Zugang zu Finanzierungskapital eine wichtige Rolle für Start-ups, aber die Gründe, warum Start-ups zu 80 bis 90 Prozent scheitern, liegen Experten zufolge eher an unternehmerischen Aspekten: fehlende fachliche und soziale Kompetenz des Gründerteams, fehlender Kundennutzen des Produkts oder des Service; ein zu kleines oder zu wenig belastbares Netzwerk; eine zu geringe Skalierbarkeit, um starkes Wachstum zu unterstützen.

Genau in diesen Aspekten sollten die Gründer stärker unterstützt werden. Mit Beratung und Coaching zum Beispiel durch erfahrene Praktiker (VOICE bietet das Start-ups mit CIOs an), flächendeckenden Enterpreneurship-Lehrgängen an den Hochschulen besonders in Ingenieur- und Informatikstudiengängen, sowie begleitenden Ausbildungsmöglichkeiten in Sachen praktischem Management und Führung. Außerdem sollte der Bund Startups in der Gründungsphase mit leicht finanzierbaren Marktstudien unter die Arme greifen.

8

Sicherheit im Internet erhöhen, „Autokennzeichen und Leitplanken für das Web".

VOICE fordert eine breit angelegte Initiative der deutschen / europäischen Politik zur Verbesserung der Sicherheit im Datenverkehr. Die Regierung muss eine starke, gestaltende Rolle in der Weiterentwicklung des Internets übernehmen.

Das Internet als bestimmendes Infrastrukturelement der modernen Wirtschaft ist in immer stärkerem Maße von organisierter Kriminalität belastet. Mit steigendem Wertschöpfungsanteil des Datenverkehrs werden die Bedrohungen zum missionskritischen Faktor für die zunehmend digitalen Geschäftsmodelle. Viele Funktionalitäten und Kommunikationskanäle mit an sich hohem Komfort für den Kunden können inzwischen aufgrund der steigenden Gefahr nicht mehr genutzt werden.[6]

Bisherige Ansätze mit Schutz der Geschäftsprozesse stellen fast ausschließlich auf Härtung der zentralen Server und der Endgeräte bzw. auf eine verbesserte Ausbildung der Anwender (Awareness-Schulung) ab. Unternehmen sind darauf angewiesen, aufwendige eigene Überwachungseinrichtungen vorzuhalten, um kriminellen Datenverkehr zu detektieren und sich dagegen zu schützen.

Bisher wurden aber noch keinerlei Maßnahmen ergriffen, um den Datenverkehr insgesamt sicherer zu gestalten. Im Gegenteil: Viele in den letzten Jahren eingeführte Funktionalitäten (Umlaute und Sonderzeichen in URLs, dynamische IP-Adress- und DNS-Namensverwaltung) haben die Gesamtsicherheit dramatisch verschlechtert.[7] Große Marktteilnehmer behelfen sich mit Spezialdienstleistern, die kriminelle Aktivitäten von Akteuren automatisiert verfolgen.

VOICE fordert die Bundesregierung auf, zusammen mit den Europäischen Partnern in der Festlegung und Normung der Protokolle im Datenverkehr eine aktive Rolle zu übernehmen und –analog zum Straßenverkehr und zum Handelsrecht- die Nachweisplichten für Kommunikationsteilnehmer (Server und Router[8]) und die Nachvollziehbarkeit der Kommunikationswege endlich zu verbessern. Zudem ist den Anwendern durch eindeutige Kennzeichnung der tatsächlichen Herkunft von Nachrichten und Dateien in Bedienoberflächen eine Beurteilung der Sicherheitslage zu erleichtern. Der Einsatz der bereits vorhandenen Sicherheitsmechanismen[9] für den Datenverkehr im WAN bzw. zwischen geografischen Zonen ist durch entsprechende Regelungen als verpflichtend festzulegen.

VOICE fordert die Bundesregierung auf, über entsprechende internationale Normungsverfahren folgende Sicherheitsmaßnahmen anzugehen:

- Einschränkung des (ohnehin ausreichend großen) Namensraumes, sodass Betrug mittels ähnlich klingender URL-Bezeichner leichter erkannt werden kann,

[6] Banken und Paketdienste können zum Beispiel mit ihren Kunden nur noch begrenzt interagieren, da (berechtigtes und unberechtigtes) Misstrauen dies torpediert.

[7] So können Angreifer mit wechselnden Serverbezeichnungen Datenflüsse leicht umlenken und durch Verwendung zum Beispiel diakritischer Zusatzzeichen (Accents etc.) täuschend ähnliche aber betrügerische URLs schaffen.

[8] Die Identitäten der betreffenden Personen sind hiervon unberührt.

[9] Wie DNSSec,STARTTLS, zertifikatbasierte Serverkommunikation etc.

- Einschränkung des Wechsels von DNS-Eintragungen zwischen IP-Adressräumen[10] (analog der Namensänderung oder des Sitzes eines Unternehmens im Handelsregister) und insbesondere die Aufnahme der Wechselhäufigkeit als Merkmal der betreffenden Domäne, sodass diese als Sicherheitsmerkmal genutzt werden kann,
- Verpflichtung der Anbieter zur eindeutigen Sichtbarmachung der Herkunft einer Nachricht in der Benutzeroberfläche, um Betrug leichter erkennbar zu machen,
- Verpflichtung der Registrare (z.B. denic für die .de-Domäne), Domänenanmeldungen im Vorhinein auf Seriosität zu prüfen (analog des Handelsregisters bzw. Post-Ident-Verfahren) und Betrugsgefahren durch Anwendung von Ähnlichkeitsmaßen bereits bei der Anmeldung einzudämmen,
- Feste Kopplung der Kennungen von Internetknoten an ihre geografische Lage, um die betrügerische Umleitung von Datenverkehr (BGP-Hijacking) auszuschließen,
- Anreicherung der Kommunikationsprotokolle mit zertifikatsbasierten Informationen zum Übertragungsweg von Datenflüssen.

Hierzu ist in einem neu zu schaffenden Bundesministerium für Digitalisierung ein dedizierter Bereich einzurichten, der die deutschen Aktivitäten in allen Normungsgremien für IT-Technologie (W3C, CEN/CLC/ETSI, ISO/IEC etc.) bündelt und koordiniert. Hierzu muss das Ministerium mit industrieunabhängigen, spezialisierten Technologieexperten bzw. mit dem Zugang zu solchen Ressourcen aus der deutschen Wissenschaft ausgestattet werden.

Weniger Bürokratie, präzisere Regeln

9

Arbeitnehmerüberlassungsgesetz (AÜG): Höchstüberlassungsdauer für Leiharbeitnehmer in der IT-Branche abschaffen.

VOICE fordert die Überarbeitung des AÜG dahingehend, dass Leiharbeitnehmer in der IT-Branche oberhalb eines festgelegten Mindeststundensatzes nicht unter die Höchstüberlassungsgrenze des Arbeitnehmerüberlassungsgesetz (AÜG) fallen.

Experten[11] gehen davon aus, dass das 2017 in Kraft getretene Arbeitnehmerüberlassungsgesetz 2023 novelliert werden muss.

Im heute geltenden AÜG ist die zeitliche Grenze für die Überlassungsdauer auf 18 Monate festgelegt. Viele erfolgskritische externe Personalressourcen in IT-Projekten müssen aber für einen erheblich längeren Zeitraum verfügbar bleiben, um unnötige Einarbeitungsprozesse und die komplizierte Auswahl immer neuer Spezialkräfte zu vermeiden. Die Höchstgrenze gefährdet die seit langem etablierte und sehr erfolgreiche Co-Innovation in der IT- und Digitalszene. Zum Teil arbeiten freie IT-Berater und freiberufliche Entwickler (gemeinsam mit festangestellten Kolleginnen und Kollegen ihrer Auftraggeber) über Jahre hinweg an einem großen IT-Projekt oder an einer Reihe kleinerer Projekte. Viele IT-Freiberufler arbeiten zudem für Personaldienstleister, die sie dann „verleihen". Die durch das Gesetz beabsichtigte Schutzwirkung für eigentlich abhängig Beschäftigte wird in diesem Bereich nicht benötigt, da eine Festanstellung regelmäßig unattraktiver ist, als die selbständige Beschäftigung.

Denn anders als Zeitarbeitskräfte in der Industrie-, Lebensmittel- und Dienstleistungsbranche verdienen freie ITler weit überdurchschnittlich. Durch die hohe Entwicklungsgeschwindigkeit und den hohen Innovationsdruck leidet der IT-Markt bereits seit Jahren unter einem starken Fachkräftemangel. Dieser wird sich durch die Digitalisierung von Wirtschaft und Gesellschaft weiter erhöhen, mit der Folge, dass die Nachfrage nach IT-Freiberuflern und IT-Beratern in den nächsten Jahren weiter ansteigen wird und diese daher weitgehend die Bedingungen für ihr Engagement selbst bestimmen können.

Die Mehrzahl der IT-Freiberufler hat den Status des „Freien" zudem bewusst gewählt. So können sie in der Regel, die Projekte auswählen, die ihnen die besten Bedingungen bieten. Außerdem gehen Freiberufler davon aus, ihre investierte Arbeitszeit besser kontrollieren zu können als festangestellte Kollegen.

IT-Freiberufler und -Berater gehören also keineswegs zu den Beschäftigten des Niedriglohnsektors, die der Gesetzgeber zu Recht schützen will.

VOICE fordert deshalb, die Höchstüberlassungsdauer des AÜG auf überdurchschnittlich bezahlte Freiberufler nicht mehr anzuwenden.
Ferner müssen die arbeitsrechtlichen Voraussetzungen geschaffen werden, damit agile Teams aus IT-Anwendern, IT-Dienstleistern und Beratern flexibel auch über längere Zeiträume zusammenarbeiten können, ohne rechtliche Risiken in Kauf nehmen zu müssen.

[10] Redundanzbedingte Wechselmöglichkeiten können vorher festgelegt und bekannt gegeben werden, willkürliche Sprünge im Sekundentakt müssen aber als Verlust an Seriosität ausgewiesen werden.

[11] https://www.arbeitsblog.de/themen/artikel/aueg-welche-aenderungen-stehen-2023-bevor/

10

Datenschutz: Illegale Nutzung wirksam verhindern, Datenverarbeitung erleichtern.

VOICE fordert, Datenschutzregelungen stärker gegen unerwünschte und missbräuchliche Analysen (z.B. Financial Scoring, Health Scoring, Persönlichkeitsprofile) auszurichten, anstatt weiterhin die Erfassung von Daten so stark einzuschränken.

Die Datenschutzgrundverordnung ist geprägt vom Prinzip der Datensparsamkeit. Dieser in Deutschland Ende der 80iger Jahr postulierte Grundsatz resultiert vor allem aus der Absicht, einem möglichen Missbrauch durch staatliche Stellen den Riegel vorzuschieben. Damals hatten Unternehmen den Wert von Daten noch nicht entdeckt. Das ist heute diametral anders. Daten sind für Unternehmen neben Kapital, Arbeit und Rohstoffen zu einem vierten Produktionsfaktor geworden und zunehmend sind sie in der einen oder anderen Form personenbeziehbar.

Ziel muss es also sein, die Verarbeitung und Nutzung dieses Produktionsfaktors auch für europäische Unternehmen zu ermöglichen und dabei die informationelle Selbstbestimmung der Bürger zu wahren und gleichzeitig Rechtssicherheit für die verarbeitenden Unternehmen herzustellen. Ansätze hierzu sind:

- Erlaubnis zu Auswertungen, wenn die Rückverfolgung der Ursprungsdaten sicher ausgeschlossen werden kann
- Kontrolle der Auswertung statt generelle Vermeidung der Verarbeitung
- Generelles Verbot von De-Anonymisierung

VOICE fordert die schrittweise Anpassung der DSGVO.

11

IT-Sicherheitsgesetz 2.0: Unterstützung statt Sanktionierung.

VOICE fordert für die Umsetzung und Anwendung des IT-Sicherheitsgesetzes 2.0 einen Fokus auf Dialog und Unterstützung anstelle Kontrolle und Sanktionierung.

Das vom Bundestag und Bundesrat verabschiedete IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) erweitert den Kreis der Unternehmen, die der sogenannten kritischen Infrastruktur (KRITIS) angehören, und verschärft zugleich die gestellten Anforderungen. Zudem skizziert es eine neue Gruppe von „Unternehmen im besonderen öffentlichen Interesse", die nunmehr einer Meldepflicht und Pflicht zur Selbsterklärung unterliegen. Neben Rüstungsunternehmen, Betrieben nach Störfallverordnung der oberen Klasse und „Unternehmen erheblicher volkswirtschaftlicher Bedeutung" werden nun auch deren Zulieferer mit „Alleinstellungsmerkmalen von wesentlicher Bedeutung" hierzu gezählt.

Die unscharfe Abgrenzung macht undifferenziert ganze Unternehmen zum Gegenstand des Gesetzes, obwohl das Risiko in einzelnen Unternehmensbereichen / Betrieben typischerweise unterschiedlich verteilt ist. Hierdurch wird den Unternehmen die Möglichkeit genommen, die Mittel zur Sicherstellung der IT-Sicherheit risikobasiert einzusetzen. Insbesondere die auferlegte Meldepflicht führt zu erheblichen Investitionen in darauf spezialisierte Systeme und rund um die Uhr verfügbares Fachpersonal zur Auswertung, die der Gesetzgeber bei der Abschätzung des Erfüllungsaufwandes der Wirtschaft augenscheinlich nicht berücksichtigt hat. Erschwerend kommt hinzu, dass Meldungen nicht nur nach einer faktischen Störung zu erfolgen haben, sondern auch sobald es zu einer solchen kommen kann. Diese Auflage geht weit über die Forderung der zugrundeliegenden NIS-Richtlinie hinaus und trägt weder zum allgemeinen Lagebild noch zur Störungsbehebung bei. Dabei wird das angedrohte Strafmaß bei Nicht-Meldung absehbar zu unnötigem Aufwand auf Seiten der Unternehmen und Behörden führen.

VOICE begrüßt die Zielsetzung der Bundesregierung, die Robustheit gegen Cyber-Angriffe für den Wirtschaftsstandort Deutschland zu erhöhen.

VOICE fordert, dass die (noch zu erstellenden) Verordnungen zur Umsetzung des IT-Sicherheitsgesetzes 2.0 die „Unternehmen im besonderen öffentlichen Interesse" und deren Zulieferer mit „Alleinstellungsmerkmalen von wesentlicher Bedeutung" zweifelsfrei und langfristig planbar definiert und ihnen den Freiraum gibt, um Mittel zur Sicherstellung der IT-Sicherheit auf Basis des Risikos zielgerichtet einzusetzen. Hierbei dürfen die Forderungen nicht unverhältnismäßig über die Forderungen der geltenden NIS-Richtlinie hinausgehen, um den Wirtschaftsstandort Deutschland nicht zu gefährden. Dabei wäre der Fokus auf Unterstützung anstelle Sanktionierung durch Behörden Grundlage einer vertrauensvollen Zusammenarbeit. Hilfreich wäre hier insbesondere eine zeitnahe und branchenspezifische Versorgung der durch die Behörden gewonnenen Informationen zu Lagebild und Schwachstellen.

12

Betriebsverfassungsgesetz: Mitbestimmungsprozess bei IT-Systemen vereinfachen

VOICE fordert die Präzisierung des § 87 Betriebsverfassungsgesetz, um Rechtsunsicherheit beim Einsatz von IT-Systemen zu beseitigen.

Die Digitalisierung der Geschäftsprozesse in der deutschen Wirtschaft muss zügig und mit möglichst geringem Gesamtaufwand erfolgen. Workflow- und Collaboration-Systeme etablieren sich zunehmend. Sie helfen mit hoher Wertschöpfung, die Betriebe auf dem

Weltmarkt konkurrenzfähig zu halten.
In der Praxis führt eine bislang uneinheitliche Rechtsprechung im Umfeld des Betriebsverfassungsgesetzes zu unnötig hohen Aufwänden im Mitbestimmungsprozess. Denn unterschiedliche Auslegungen des § 87 BetrVG führen dazu, dass jede einzelne IT-Komponente als mitbestimmungspflichtig angesehen werden kann.[12] Mit zunehmender Durchdringung der Prozesse mit IT führt dies zu immer höherem Abstimmungsaufwand mit hohen zeitlichen Risiken. Über kurz oder lang wären alle Geschäftsprozesse vollständig mitbestimmungspflichtig.

Ähnlich anderer Rechtsbereiche (Arbeitssicherheit, Brandschutz etc.) muss deshalb die Mitbestimmung auf Funktionen beschränkt werden, die auch den entsprechenden Gestaltungsspielraum aufweisen. So kann z.B. die Konfiguration von Präsenzanzeigen Gegenstand der Verhandlung sein. Für den Normalbetrieb von IT-Werkzeugen und Anwendungen muss der Umgang und die Administration so geregelt werden, dass Verhandlungen darüber unnötig werden.

VOICE fordert deshalb eine Präzisierung und Detaillierung dahingehend, welche Systemfunktionen und Auswertungsmethoden erlaubt bzw. welche verboten sind. Dies muss keinesfalls mit der Einschränkung von Arbeitnehmerrechten einhergehen. Im Gegenteil: VOICE unterstützt in der modernen Wissensgesellschaft ausdrücklich Führungsmethoden, die auf Kreativität und Eigenverantwortung setzen. Verhaltenskontrolle ist – insbesondere im Kontext zunehmender Remote-Arbeit - generell als veraltete Führungsmethode anzusehen. Dies ist ein Grund mehr, bei dem bestehenden Digitalisierungsdruck auf ausufernde Verhandlungen mit den Mitbestimmungsgremien so weit wie möglich zu verzichten.

[12] Der Passus „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen." wird dabei in der Rechtsprechung teilweise sehr weitgehend interpretiert. So kann selbst ein einfacher Login-Vorgang bei einer SaaS Anwendung als im Sinne des §87 BetrVG für eine Verhaltenskontrolle nutzbarer Schritt gesehen werden. Siehe Dauerbrenner: Software vs. Mitbestimmung https://www.luther-lawfirm.com/newsroom/newsletter/detail/newsletter-arbeitsrecht-1-ausgabe-2021#acc-3

IMPRESSUM

VOICE
CIO Bundesverband der IT-Anwender e.V.

VOICE – Bundesverband der IT-Anwender e.V.
Invalidenstraße 91, 10115 Berlin Berlin
Tel.: +49 30 2084 964 70
Fax: +49 30 2084 964 79
E-Mail: voice-info@voice-ev.org

USt-IdNr: DE 281638339
VR 31149 B Berlin Charlottenburg

Vertreten durch:

Dr. Bettina Uhlich
Vorsitzende des Präsidiums

Dr. Hans-Joachim Popp
Stellvertretender Vorsitzender des Präsidiums

Thomas Rössler
Stellvertretender Vorsitzender des Präsidiums

Geschäftsführer und verantwortlich für den Inhalt nach § 55 Abs. 2 RStV: Wolfgang Storck

Veröffentlicht:
Berlin, den 15.06.2021