VOICE Bundesverband der IT-Anwender e.V.

14 Forderungen zur Konkretisierung der Cyber-Sicherheitsstrategie für Deutschland 2016

Vorgelegt von
VOICE – Bundesverband der IT-Anwender e.V.
im März 2017

Unter maßgeblicher Beteiligung von
Dr. Hans-Joachim Popp
Präsidiumsmitglied für den Bereich IT-Security

VOICE - Bundesverband der IT-Anwender e.V. unterstützt die vom Bundesministerium des Inneren im November 2016 vorgelegte Cyber-Sicherheitsstrategie ausdrücklich. Damit die digitale Transformation der Wirtschaft gelingen kann, wird ein hohes Maß an Cyber-Sicherheit benötigt, zu dem alle Beteiligten ihren Beitrag leisten müssen. Die Anwenderunternehmen, gerade solche, die kritische Infrastrukturen betreiben, müssen ihrer Verantwortung klar gerecht werden und Sicherheitsvorgaben und -maßnahmen in ihren Unternehmen – naturgemäß im Einklang mit den sonstigen Regelungen – konsequent und nachhaltig etablieren. Anbieterunternehmen müssen ihren Produkten und Services mehr Eigensicherheit geben und die Haftung für die sicherheitsbezogenen Eigenschaften übernehmen. Das allseits verwendete Stichwort " Security by Design" ist konkret mit Leben zu füllen. Die Politik ist ebenfalls gefordert. Sie muss die Rahmenbedingungen setzen und den Gesetzesrahmen so umgestalten, dass Kommunikations- und Geschäftsbeziehungen in der digitalen Welt genauso geschützt sind, wie dies in der physischen Welt heute der Fall ist, ohne dabei den legalen und gewollten Datenverkehr einzuschränken. Hier agiert die Politik auf nationaler und auf internationaler Ebene aus Sicht von VOICE bislang noch viel zu zurückhaltend. Vom Grundsatz her muss im digitalen Raum das gleiche Recht und der gleiche Schutz gelten wie in der analogen Welt. Von diesem Grundgedanken getragen, hat VOICE die nachfolgenden 14 Forderungen formuliert, die die Cyber-Sicherheitsstrategie der Bundesregierung ergänzen sollen.

#1: Digitale Kommunikations- und Geschäftsbeziehungen darf in Deutschland/EU nur eingehen, wer sich an die geltenden gesetzlichen Regeln hält.

Da die internet-basierte Kommunikation und darauf aufbauende Geschäftsprozesse für jeden Einzelfall die Kooperation beider Partner erfordert, ist eine selektive Ablehnung von (im Sinne der Cyber-Sicherheit) mangelhaften Beziehungen (z.B. im Fall fehlender Konformität zu in Deutschland herrschenden Transparenz- und Authentisierungsbedingungen eines der Partner) leicht zu bewerkstelligen und somit als Durchsetzungsinstrument für als sinnvoll erkannte Schutzmaßnahmen sehr wohl in Erwägung zu ziehen. Hier sollten Analogien aus dem zivilen Leben als Beispiele mit einbezogen werden. Wo Verstöße gegen bereits heute geltendes Recht bislang nur schwer nachzuweisen sind, muss der Staat schnell in die Lage versetzt werden, die Nachweise schneller und konsequenter zu erbringen. Bis dahin sind solche schwer entdeckbaren Verstöße innerhalb des vorhandenen Rechtsrahmens unter Nutzung des höchstmöglichen Strafmaßes zu ahnden. Fehlende Sanktionierungsmöglichkeiten müssen zügig ergänzt werden, um das Vertrauen der seriösen Nutzer in die digitalen Prozesse zu stärken.

#2: Mehr digitaler Anwenderschutz. Dieser muss für klare, verständliche, Anwender orientierte Regeln und ihre Durchsetzung sorgen. Außerdem muss der Anwender in der digitalen Welt beim Schutz gegen schädliche Einflüsse unterstützt werden.

So ist schon heute auch für Anwender mit hoher Vorbildung und optimaler Aufmerksamkeit eine Durchdringung aller seiner Interaktionen mit Web-basierten Systemen nicht mehr erreichbar. Diese Tendenz wird sich verstärken. Konsequenterweise muss die notwendige Transparenz durch Komplexitätsreduktion oder - wo dies nicht möglich ist - durch gezielte Schaffung von leicht aufnehmbaren Situations- und Ablaufdarstellungen erreicht werden. Ähnlich wie in vielen sonstigen Wirkungsfeldern, in denen der Mensch über keine ausreichende Sensorik verfügt (Beispiel Strahlenschutz, Spurenelemente in Lebensmittel, Schadstoffe in der Umwelt) ist absehbar, dass eine gezielte Unterstützung des Bürgers und der Wirtschaft beim Eigenschutz gegen schädliche Einflüsse erforderlich wird. Wie im „analogen“ Leben (siehe GmbH-Recht, Notariatsverträge für Immobilienkäufe, Zulassungsprozeduren für gefahrenträchtige Produkte etc.) muss dies durch Regularien zur Erzwingung der Transparenz erreicht werden (-> Verbraucherschutz).

#3: Die heutige Generation von Führungskräften in Politik und Wirtschaft muss ihre Kompetenzlücke im Bereich IT-Security nachweislich schließen.

Der Kompetenzaufbau für Bürgerinnen und Bürger muss gefördert werden, jedoch ist mit dem natürlichen Generationenwechsel ein Aufbau vieler Teilkompetenzen allein schon durch die Bekanntschaft mit digitalisierten Prozessen im frühen Kindesalter zu erwarten. So kann eine gezielte Ausbildung im Bereich der Handhabungskompetenz für IT-Systeme innerhalb weniger Jahre obsolet werden. Die wesentlich gravierendere Kompetenzlücke besteht in der jetzigen Generation der Führungskräfte in Politik und Wirtschaft. Sie ist mit den kurzfristig anstehenden Weichenstellungen, deren Auswirkungen - im Positiven wie im Negativen - kaum absehbar sind, weitgehend überfordert. Notwendig ist daher eine schnelle und umfassende Ausbildung dieser Kräfte in Fragen der IT-Sicherheitsarchitektur und der Begleiteffekte (auf dem derzeitigen Wissensstand der Fachwelt). Das Erreichen einer eigenständigen Beurteilungsfähigkeit ist erfolgskritisch für die Implementierung der Digitalen Agenda in der Gesellschaft. Das hierfür erforderliche Selbstbewusstsein der „Digital Immigrants“, also der älteren Mitbürger, ist gezielt zu fördern. Die Medienkompetenz (für die es auf allen Seiten, vor allem aber bei den jüngeren Generationen große Defizite gibt) ist von der Handhabungskompetenz (bei der es für jüngere Nutzer so gut wie keinen, für ältere nur geringen Nachholbedarf gibt) getrennt zu sehen.

#4: Security by Design muss bei allen digitalen Produkten Standard sein.

Die vielzitierte Sensibilität der Anwender in Bezug auf Sicherheitsfragen muss gestärkt werden. Entscheidend ist aber langfristig die „Eigensicherheit“ der Produkte und Service. Selbst bei größter Sensibilität reicht die normale Vorbildung eines Anwenders bzgl. Security nicht aus, um Sicherheitslücken zu erkennen oder sogar zu schließen. Deshalb müssen Anwender auf Websites jederzeit nachvollziehen können, in welcher Kommunikationssituation (insbesondere bzgl. der Quellen der präsentierten Informationen) sie sich befinden. Als Teil des Ansatzes Security-by-Design muß die Unterstützung des Menschen im Gesamtprozess ein essentieller Bestandteil sein.

#5: Sichere elektronische Identitäten müssen besser als bisher geschützt werden. Ihre konsequente Anwendung sollte durch intuitive, aber dennoch robuste Authentisierungsprozesse erleichtert werden.

Die Bedeutung dieses Arbeitsgebiets kann in seinem Einfluss auf das Gesamtergebnis nicht hoch genug eingeschätzt werden. Die Verfahren für eine sichere Identität beschränken sich aber nicht auf die Verbesserung des Authentisierungsvorgangs selbst. Sie müssen vielmehr auch die sachgerechte Verwaltung und Verwahrung der zugehörigen Authentisierungsmerkmale und eine entsprechende Granulierung der resultierenden Lese- und Schreibrechte berücksichtigen. Dies ist mit Blick auf die Bedeutung des betreffenden Geschäftsprozesses aktiv und differenziert zu gestalten.

#6: Für digitale Produkte müssen die gleichen Produkthaftungsregeln gelten wie für gegenständliche Produkte. Das gilt insbesondere für die Einhaltung der Datenschutzregularien.

Die Produkthaftungsregeln müssen auf digitale Produkte ausgeweitet werden. Dabei dürfen die bereits in der „analogen" Welt geltenden Regeln nicht aufgeweicht werden. Hersteller und Betreiber müssen insbesondere bzgl. des Schutzes der neu entstehenden, massiven Volumina personenbezogener bzw. personenbeziehbarer Daten in die Pflicht genommen werden.

#7: Sicherheitsforschung muss intensiviert werden.

Die in den verschiedenen Kompetenzzentren durchgeführten Projekte sollten genauer koordiniert und fokussiert werden. Dabei sollten die Schwerpunkte auf der Erzeugung von Transparenz in der Benutzerinteraktion, der vereinfachten Bedienung von Schutzmechanismen sowie auf dem Schutz großer Datenmengen vor unbefugten internen und externen Zugriffen liegen. Der bisherige Schwerpunkt der Sicherheitsforschung auf Perimeterschutz sollte ergänzt werden um Themen wie Security Analytics und Adaptive Security Infrastructure.

#8: Deutsche und europäische IT-Anbieter sollten gefördert werden, um auch international in Sicherheitsfragen auf Augenhöhe zu bleiben.

Die Förderung der deutschen und europäischen Anbieter sollte sich nicht auf IT-Security-Themen beschränken. Der Auf- und Ausbau von Know-how bei deutschen und europäischen Anbietern im gesamten Bereich der IT-Infrastruktur (mit dem Schwerpunkt auf Netz- und Serversystemen bis hin zu Applikationen) ist essentiell für die Wahrung der „Augenhöhe“ auch im Bereich der IT-Sicherheit. Ausgehend von der Tatsache, dass nicht alle Sicherheitslücken in marktgängigen Produkten durch Zusatzsysteme absicherbar bzw. behebbar sind, muss auch für die Europäische Wirtschaft die Möglichkeit geschaffen werden, Produkte zu beziehen, die einem erhöhten Sicherheits- und Datenschutzniveau entsprechen (z.B. durch besonders konsequenten Einsatz von Security-by-Design) als dies in anderen Wirtschaftsräumen derzeit noch gefordert ist. Der erforderliche Produktreifegrad kann nur durch Einsatz und Erprobung der Systeme in einem den Anbietern positiv gegenüberstehenden Anwenderumfeld erreicht werden. Dies muss durch die Regierungsstellen folglich gezielt gefördert werden.

#9: Das nationale Cyber-Abwehrzentrum sollte konkrete Schutzfunktionen übernehmen, um lokale Maßnahmen effizienter zu erbringen.

Das Cyber-Abwehrzentrum muss in seinem Tätigkeitsfeld weiterentwickelt werden und - wie in der Strategie der Bundesregierung vorgesehen – mit eigenen Bewertungs- und Auswertungsfähigkeiten ausgestattet werden. Darüber hinaus sollte perspektivisch auch die Wahrnehmung von konkreten Schutzfunktionen in Erwägung gezogen werden. In Betracht zu ziehen ist die einrichtungsübergreifende Bereitstellung von Detektions- und Sperrfunktionen für Unternehmensgruppen und Verwaltungsverbünde. Die bislang weitgehend lokal erbrachten Schutzfunktionen könnten so effizienter und vor allem konsequenter erbracht werden. So kann eine bekannte Quelle für Schadsoftware (z.B. www.paypal.de.sichererer-bezahlen.ru) für alle deutschen Internet-Teilnehmer zentral gesperrt werden, anstatt die jeweiligen Sicherheitsverantwortlichen nur darüber zu informieren, dass eine Adresse gefährlich ist. Die Zeit zwischen dem Auftreten einer Bedrohung und der zugehörigen Abwehrreaktion könnte so deutlich verkürzt werden. Ggf. hierfür erforderliche gesetzliche Anpassungen (TMG, TKG etc.) sollten nicht zu defensiv angegangen werden.

#10: Es müssen wirksame Nachweismethoden für Datenflüsse entwickelt werden, um Aufklärungsarbeit und Strafverfolgung im nationalen und internationalen Cyber-Raum zu verbessern.

Die in der Cyber-Sicherheitsstrategie der Bundesregierung beschriebenen Ziele einer verstärkten Bekämpfung von Cyber-Kriminalität sind uneingeschränkt zu unterstützen. Entscheidend für die erfolgreiche Aufklärung von Straftaten unter Nutzung des Internets wird aber vor allem die Etablierung wirksamer Nachweismethoden für Datenflüsse sein. Bislang gibt es hierfür praktisch keine Grundlagen. Entsprechend aufwendig und teuer, gleichzeitig aber auch von Unschärfen bestimmt, ist heute die Aufklärungsarbeit durch Spezialisten. Die Etablierung solcher Nachweisstrukturen (im „analogen" Leben sind sie am ehesten mit der KFZ-Kennzeichenpflicht, dem Fahrtenschreiber bei LKW, dem Handelsregister oder der forensischen DNA-Analyse zu vergleichen) ist eine supranationale Aufgabe. Die Anstrengungen in diesem Bereich sollten dringend verstärkt werden. Im Ergebnis würden einerseits erhebliche Ermittlungsaufwände eingespart und aufgrund der letztlich erhöhten Aufklärungsquote ein neues Abschreckungspotenzial für die bislang völlig risikolos arbeitenden cyber-kriminellen Organisationen erschlossen.

#11: Die Integrität der Software aller in kritischen Infrastrukturen eingesetzten Endgeräte muss fortwährend überwacht werden, um unerlaubte Modifikationen zu erkennen.

Die Verhinderung von Informationsabflüssen im Zuge von Spionageakten muss Priorität vor der Beschäftigung mit Sabotage-Akten haben. Grund hierfür ist die Problematik, das unentdeckte Aktivitäten ein erheblich höheres Gefahrenpotential bergen, da die Sichtbarkeit und die Nachvollziehbarkeit für politische Entscheider fehlen und damit der Weg zu wirksamen Gegenmaßnahmen beschwerlich ist. Unmittelbar ausgeführte Sabotageakte führen kurzfristig zur Durchsetzung von massiven Abwehrmaßnahmen. Eine besondere Gefahr geht von Sabotageakten aus, deren Planungsphase über lange Zeit unentdeckt bleiben und die deshalb einen besonders großen Schaden entfalten können (ein Szenario im Bereich der KRITIS wäre die Infiltration eines grundlegenden, flächendeckend eingesetzten Kommunikationsmechanismus, der auf ein externes Schaltkommando hin sein Verhalten ändert und so eine Krise auslöst. Ein konkretes Beispiel aus jüngster Zeit ist der Manipulationsversuch an 800 000 Routern von Kunden der Telekom Deutschland). Um solchen Szenarien entgegenzutreten, wird die kontinuierliche und vollständige Kontrolle der Softwarestände aller beteiligten Endgeräten unumgänglich sein. Um dies handhabbar zu machen, sind massive Anstrengungen im Betrieb der Systeme aber auch in der Erforschung neuer Werkzeuge notwendig.

#12: Die Bundeswehr muss Strukturen entwickeln, um die Infrastrukturen des Landes zu schützen und die Resilienz der Verteidigungssysteme bezüglich Cyber-Angriffen zu erhöhen.

Die vorgesehenen Maßnahmen zum Aufbau einer Cyber-Abwehr als Teildisziplin der Bundeswehr sind dringend notwendig. Dabei ist nicht nur der Schutz der Infrastruktur des Landes zu beachten, sondern auch die gerade im Hinblick auf die sich verschärfende Sicherheitslage hohe Verletzlichkeit der konventionellen Verteidigungssysteme. Einem hybriden Angriff (Cyber- und konventionelle Methoden in Kombination) könnte die Bundeswehr derzeit nur sehr eingeschränkt begegnen. Die Resilienz des Verteidigungssystems gegen Cyber-Angriffe muss im Detail überprüft und ggf. zügig passende Sicherheitsmaßnahmen ergriffen werden.
Mit einer zunehmenden Vermischung von Fragen der inneren mit der äußeren Sicherheit werden der Bedarf nach gegenseitiger Unterstützung der jeweils zuständigen Behörden und gleichzeitig die möglichen Synergieeffekte immer stärker. Dem muss durch eine Anpassung der Vereinbarungen zur Zusammenarbeit und ggf. auch der rechtlichen Regelungen Rechnung getragen werden.

#13: Es müssen wirksame national und international geltende Regularien geschaffen werden, um Straftaten im Cyber-Raum zu unterbinden.

Die bisherige Sicherheitspolitik bezieht sich derzeit in erster Linie auf die Regulierung empfohlener bzw. mandatorischer Schutzmaßnahmen, angepasst an die jeweilige Kritikalität eines Netzteilnehmers. Damit wird zwar die Fähigkeit zum Eigenschutz erhöht, aber bislang fehlt es an systemischen Regularien zur wirksamen Unterbindung von Straftaten im Cyber-Raum (Sinnbilder: Autokennzeichen zur Unterstützung der Verbrechensbekämpfung, Waffengesetze zur Begrenzung und Zugangssteuerung der überhaupt verfügbaren Tatwaffen). Die hierfür notwendigen Regularien sind aufgrund des bislang (insbesondere im internationalen Datenverkehr) sehr begrenzten Einflusses deutscher und europäischer Institutionen nur rudimentär vorhanden. Mit steigender Transparenz des Datenverkehrs wird automatisch auch die Abwehrfähigkeit Deutschlands und Europas im Cyber-Raum gestärkt, da insbesondere Angriffe mit Vorbereitungscharakter schneller entdeckt und abgewehrt werden können.

#14: Es müssen verbindliche Sicherheitsregeln für den internationalen Datenverkehr geschaffen werden. Länder, die das Regelwerk nicht akzeptieren, werden entsprechend kontrollierter und eingeschränkter am Datenverkehr be-

Die Verbesserung der Cyber-Sicherheit muss durch die Einführung von Regelungen analog anderer Lebensbereiche vorangetrieben werden. Da Kommunikation im Cyber-Raum stets die Kooperation beider Partner sowie der ggf. dazwischen liegenden Partner mit Brückenfunktion erfordert, kann die Durchsetzung von Anforderungen der Europäischen Partner sehr wohl gelingen. Partner, die nicht bereit sind, Minimalanforderungen zu akzeptieren, können bzgl. des Datentransfers auf einfache Weise anders behandelt werden, als solche mit regelkonformer Organisation der lokalen Verwaltungseinheiten für die Internet-Kommunikation. Länder mit staatlich akzeptiertem, jedoch nach europäischem Recht ungesetzlichem Verkehrssteuerungsverhalten (z.B. sog. DNS-Poisoning) könnten mit entsprechenden zusätzlichen Informationen für Europäische Kommunikationspartner versehen werden. Je nach Anlass und Schutzbedarf der Kommunikation können die Europäischen Partner dann reagieren. Die Gründung eines Instituts für Internationale Cyber-Sicherheit ist uneingeschränkt zu unterstützen. Ein Regelwerk zur Verhinderung von Missbrauch im Internet muss umgehend aufgestellt und –ggf. auch einseitig- aktiviert werden.

Impressum

VOICE - Bundesverband der IT Anwender e.V.

Vertreten durch:

Dr. Thomas Endres	Vorsitzender des Präsidiums
Dr. Ralf Schneider	Stellvertretender Vorsitzender des Präsidiums
Constantin Kontargyris	Stellvertretender Vorsitzender des Präsidiums
Dr. Hans-Joachim Popp	Präsidiumsmitglied für den Bereich IT-Security

Büro Berlin:	Kurfürstendamm 217, 10719 Berlin
Büro München (Postanschrift):	Hohenlindener Str. 1, 81677 München
Büro Köln:	Waltherstr. 49-51 Haus 1, 51069 Köln

Tel.:	+49 30 2084 964 70
Fax:	+49 30 2084 964 79
E-Mail:	voice-info@voice-ev.org

Umsatzsteueridentifikationsnummer:	DE 281638339
Registergericht:	Berlin Charlottenburg
Vereinsregisternummer:	VR 31149 B

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