Norbert Pohlmann

Zur Entwicklung einer IT-Sicherheitskultur

Wie das IT-Sicherheitsgesetz den gesellschaftlichen Umgang mit IT-Risiken fördern kann.

Die Erkenntnis ist bitter: Der Umgang mit Informationstechnologien wird fortlaufend durch Angriffe bedroht, deren Schadenswirksamkeit steigt. Diese Tendenz kann auch durch aufwendige technologische Entwicklungen nicht aufgehalten werden. Ein Ausweg aus dem Dilemma scheint eine bewusste Neuorientierung der Gesellschaft zu sein. Im Beitrag werden dafür Anregungen entwickelt, die eine IT-Sicherheitskultur als Teil einer Lösung empfehlen.

1 Ausgangssituation

Die Informationstechnologien und das Internet spielen in unserer Gesellschaft eine immer wichtigere Rolle. Im Juli 2015 waren bereits 52,86 Mio. Menschen in Deutschland online [1].
Wir suchen und finden wichtige Informationen, wie Nachrichten, Fakten, Wissen, usw. im Internet. Soziale Kontakte pflegen wir zunehmend ebenfalls im Internet, wir kaufen immer häufiger im Internet ein und unsere Behördengänge finden immer öfters im Internet statt. Es findet insgesamt eine umfangreiche Digitalisierung unseres Lebens statt. Wir realisieren mit immer intelligenteren IT-Endgeräten (Smartphones/ Wearables, …) unsere Arbeitsabläufe mit und über das Internet. Immer mehr Daten und Anwendungen von Firmen liegen im Internet, wie Cloud-Dienste, Internet-Storages, usw. und immer mehr intelligente Algorithmen im Internet verarbeiten personenorientierte Sensordaten im Internet (Big-Data, Smart-Data, …). Industrie 4.0 bringt die Industrieanlagen für den optimalen Betrieb auch ins Internet und mit dem Internet der Dinge werden alle „Dinge", wie Kühlschrank, Toaster, usw. im Internet verfügbar und ansprechbar sein. Aber, um es mit den Worten Goethes zu sagen: „Wo viel Licht ist, ist auch viel Schatten."

Wir müssen nüchtern realisieren, dass unsere IT und IT-Sicherheitstechnologien heute nicht sicher und vertrauenswürdig genug sind. Das heißt, die Widerstandsfähigkeit gegen professionelle Angreifer ist nicht ausreichend. Professionelle Hacker greifen alles erfolgreich an, wie wir jeden Tag aus den Medien erfahren. Das Risiko wird jedes Jahr größer und die Schäden für jeden einzelnen Bürger, für jede Firma und für unsere Gesellschaft auch!

Norbert Pohlmann

Professor für Informationssicherheit und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälische Hochschule Gelsenkirchen sowie Vorstandsvorsitzender des TeleTrusT – Bundesverband IT-Sicherheit.
E-Mail: pohlmann@internet-sicherheit.de

2 Die aktuelle Sicht auf die unsichere IT

In den folgenden Abschnitten werden die gesellschaftlichen Herausforderungen im Bereich der IT- und Internet-Sicherheit beschrieben und diskutiert [2].

2.1 Privatsphäre und Datenschutz

Der Aspekt Privatsphäre spielt für jeden Bürger eine sehr wichtige Rolle. Eine Gesellschaft, die wirtschaftlich und politisch auf die Eigenverantwortlichkeit des Einzelnen setzt, muss umgekehrt das schützen, was den einzelnen als Sozialwesen und als Wirtschaftsfaktor ausmacht: Einerseits seine persönliche Integrität und andererseits seinen materiellen Besitz. Wenn wir als Gesellschaft nicht mehr in der Lage sind, diese Anforderungen zu erfüllen, dann verlieren wir einen Teil der Demokratie und geben unsere Freiheit auf. Unsere gesellschaftlichen Reaktionen in der Summe sind, bezogen auf die Schwere des Angriffes auf unsere Privatsphäre, der überwiegend durch die NSA und die unterstützenden US-Internet-Marktführer durchgeführt wird, lächerlich, bezogen auf die Schäden für unsere Gesellschaft. Eine offene und aktive Diskussion darüber, wie der Datenschutz und die Privatsphäre in der Zukunft gestaltet werden kann und muss sowie welche Rolle sie spielen sollen, wird intransparent eher hinter geschlossenen Türen von einigen wenigen Fachleuten geführt. Das vernichtende Urteil bezüglich „Safe Harbor" unterstreicht nochmals die Notwendigkeit, jetzt aktiv zu handeln.

2.2 Selbstbestimmung und Autonomie

Internet-Dienste machen Handlungsvorschläge für uns Nutzer auf der Basis verschiedener Arten von Sensoren, wie Wareables, Smartphones, Internet-Dienste, usw. Intelligente Algorithmen nutzen diese vielen privaten Sensordaten, bewerten diese, vergleichen sie mit privaten Daten von anderen Menschen und nutzen allgemeines Wissen und Erfahrungen, um Handlungsempfehlungen für uns Nutzer zu berechnen. Das kann für uns sehr nützlich sein, bezogen auf eine gute Entscheidung für eine Handlung. Der individuelle Mensch mit seinem persönlichen Wissen, Erfahrungen und seine Intuition sowie zusätzlich intelligente Algorithmen mit sehr vielen Daten und fast unbegrenzter Rechnerpower sind ein optimale Ergänzung.

Wenn die Internet-Dienste das für uns transparent machen, sind gut berechnete Handlungsempfehlungen für unsere optimale Handlungsentscheidung sehr hilfreich.

Wenn die Internet-Dienste aber mit solchen Diensten indirekt Geld verdienen, wird die berechnete Handlungsempfehlung eher im Interesse des Internet-Dienstes und dessen Kunden liegen, als im Interesse der Nutzer. Jeder Nutzer wird zwangsläufig zum Produkt. Das Problem dabei ist, dass wir unsere Selbstbestimmung verlieren und Marionetten der Internet-Dienste werden. Das können wir als moderne Gesellschaft nicht wollen.

2.3 Wirtschaftsspionage

Die Wirtschaftsspionage ist eine weitere gesellschaftliche Herausforderung. 100 Milliarden Euro Schaden im Bereich der Wirtschaftsspionage im Jahr laut dem Verein Deutscher Ingenieure (VDI). Die Schäden beinhalten insbesondere Umsatzeinbußen von 23 Milliarden Euro durch Plagiate, Kosten von 18,8 Milliarden Euro durch Patentrechtsverletzungen und Verluste durch Ausfall, Diebstahl oder Beeinträchtigen von IT-Systemen sowie Produktions- und Betriebsabläufen von 13 Milliarden Euro.

Diesen hohen Betrag an Schaden können wir uns als Wissensgesellschaft nicht leisten! Die Angreifbarkeit unserer IT wird immer größer und unsere Werte, die als Bits und Bytes zur Verfügung stehen, werden immer risikobehafteter. Hier müssen wir umgehend aktiv werden und mit den unterschiedlichen Stakeholdern zusammen geeignete, gemeinsame IT-Sicherheitsmaßnahmen einleiten, um unsere Werte als Wissensgesellschaft deutlich wirkungsvoller zu schützen. Diese Angelegenheit muss auf allen Ebenen zur Chefsache werden.

Der Bereich Internet-Kriminalität mit z.B. erfolgreichen Angriffe auf Online Banking und Distributed Denial of Service (DDoS) Angriffen, verursacht jährlich einen Schaden von ca. 100 Mio. Zusätzlich sollten wir hier beachten, dass die Dunkelziffer in diesem Bereich sehr hoch sein wird. Insbesondere der Bereich DDoS und Erpressungen mit der Androhung von DDoS, ist zurzeit ein lukrativer Bereich für kriminelle Organisationen [3].

2.4 Cyber War

Eine weitere und immer bedeutsamere Herausforderung ist Cyber War. Angriffe auf Kritische Infrastrukturen, wie die Energieversorgung, stellen eine prinzipiell höhere Angreifbarkeit unserer Gesellschaft dar und sind eine weitere wichtige Herausforderung unserer Gesellschaft.

Mit Stuxnet haben wir lernen müssen, dass mit einem Kostenaufwand von rund 9 Mio. US Dollar für eine intelligente Malware politische Ziele einfach und sehr erfolgreich umgesetzt werden können. Mit der intelligenten Malware Stuxnet haben die Amerikaner und Israelis zusammen die Uran-Aufbereitung im Iran um zwei Jahre verzögern können.

Die schreckliche Alternative dieses politischen Zieles wäre gewesen, dass über 200.000 Soldaten in den Iran einmarschiert wären, was nicht nur Kosten von mehreren Milliarden US Dollar verursacht, sondern auch Menschenleben aufs Spiel gesetzt hätte. Wir müssen uns auf diese neue Wirklichkeit von Cyber War professionell einstellen.

Dieser erfolgreiche Angriff im Iran ist im Grunde genommen auch auf Deutschland übertragbar, denn mit dem Ausstieg aus der Atomenergie haben wir als Gesellschaft einen mutigen Weg eingeschlagen. Der Atomausstieg sorgt hier z.B. für mehr Risiko in der Energieversorgung, da jetzt die Stromnetze und deren Komponenten vernetzt werden, um intelligenter, d.h. effizienter zu werden. Dadurch steigen das Risiko einer Unterbrechung der Stromversorgung und damit die Funktionsfähigkeit unserer Gesellschaft durch Internet-Angriffe erheblich. D.h. wir müssen dafür sorgen, dass unsere Energieversorgung und die anderen Kritischen Infrastrukturen für unsere Gesellschaft sicher und robust gegen Cyber-Angriffe werden.

2.5 Evaluierung der IT-Sicherheitssituation

Wir kennen die IT-Sicherheitsprobleme, doch die heute vorhandenen und genutzten IT-Sicherheitssysteme und IT-Sicherheitsmaßnahmen reduzieren das IT-Sicherheitsrisiko nicht ausreichend! Es handelt sich um ein globales Problem, und die zukünftigen Angriffe werden die heutigen Schäden noch deutlich überschreiten.

Wir brauchen innovative Ansätze im Bereich der Internet-Sicherheit, um das Risiko für unsere Gesellschaft auf ein angemessenes Maß zu reduzieren.

Wir müssen realisieren, dass unsere Herausforderungen nicht trivial sind, und wenn jetzt nicht die unterschiedlichen Stakeholder zusammen eine gemeinsame IT-Sicherheitsstrategie definieren und passende IT-Sicherheitsmaßnahmen einleiten, wird die Nutzung des Internets mit all seinen innovativen Diensten immer problematischer, was die Wachstumschancen unsere Wirtschaft erheblich gefährdet.

3 IT-Sicherheitskultur

Die IT-Sicherheitskultur und das Verhalten einer Gesellschaft bedingen sich gegenseitig. Die IT-Sicherheitskultur beschreibt z.B. wie mit den Fragen zur IT-Sicherheit umgegangen wird. Sie unterliegt einem komplexen Lernprozess, in dem sich gemeinsame Ziele, Interessen, Normen, Werte und Verhaltensmuster in einer Gesellschaft herausbilden.

Die Wertvorstellungen in Bezug auf schützenswerte IT-Güter und IT-Sicherheitsmaßnahmen sind in den unterschiedlichen Staaten verschieden und schlagen sich in den nationalen Gesetzen und Normen nieder. Sie geben somit auch Aufschluss über die nationale IT-Sicherheitskultur eines Landes.

3.1 Kulturelle Unterschiede

Das Internet ist global und geht über alle Grenzen und Kulturen hinaus. Es gibt insbesondere im E-Commerce unterschiedliche Auffassungen darüber, was richtig und was falsch ist. Die Unsicherheiten, die durch verschiedene Rechtssysteme entstehen, müssen im täglichen Leben berücksichtigt werden.

Unterschiedliche Staaten haben z.B. sehr unterschiedliche Wertvorstellungen in Bezug auf private Daten. Die Antworten auf eine Frage an Internet-Nutzer zeigt dies ganz deutlich: Gehören private Daten, die von einem Internet-Dienstanbieter gesammelt werden, der Firma (z.B. Facebook)?

In USA sagen 76 % der Nutzer, ja diese Daten gehören dem Internet-Dienstanbieter, z.B. Facebook. In Deutschland sagen nur 22 %, diese Daten gehören der Firma.

Wir müssen diese kulturellen Unterschiede schon sehr ernst nehmen, da die wichtigsten Internet-Marktführer aus den US kommen. Das bedeutet, dass die meisten IT-Produkte und IT-Dienste nicht den kulturellen Anforderungen in Deutschland genügen.

3.2 Regulierte IT-Sicherheitskultur

Die unterschiedlichen IT-Sicherheitskulturen haben sich im Laufe der Zeit entwickelt und stellen die aktuellen Wertevorstellungen unserer Gesellschaften dar.

In Deutschland haben wir im IT-Sicherheitsbereich insbesondere das Gesetz der Digitalen Signatur, das in diesem Jahr von der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) [4] ersetzt wurde und ein Bundesdatenschutzgesetz, das im nächsten Jahr durch die EU-Datenschutzverordnung abgelöst werden soll. Ganz neu hinzugekommen ist diesen Sommer das „IT-Sicherheitsgesetz", das über die nächsten Jahre seine Wirkung entfalten wird. Aber auch dieses Gesetz soll durch die europäische Netzwerk-Informationssicherheits-Richtlinie (NISD) in Europa in naher Zukunft „vereinheitlicht" werden.

4 IT-Sicherheitsgesetz

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist am 25.07.2015 in Kraft getreten.

Das IT-Sicherheitsgesetz soll die Sicherstellung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit informationstechnischer Systeme (IT-Sicherheit) gewährleisten. Aspekte des IT-Sicherheitsgesetztes sind: Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit für Betreiber Kritischer Infrastrukturen sowie zur Meldung erheblicher Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI), Gewährleistung des Fernmeldegeheimnisses, des Schutzes personenbezogener Daten sowie der Verfügbarkeit der Datenverarbeitungssysteme durch die Telekommunikationsanbieter, Überprüfung der Sicherheitskonzepte durch die Bundesnetzagentur, Benachrichtigung der Nutzer über Sicherheitsvorfälle, Vorlage eines Jahresberichts, Festschreiben des BSI als Zentralstelle für IT-Sicherheit und die Stärkung des BKA im Bereich Cyberkriminalität.

5 Notwendige Entwicklungen

Im Folgenden werden beispielhaft einige Felder aufgezeigt, in denen sich international gemeinsame Ziele, Interessen, Normen, Werte und Verhaltensmuster entwickeln müssen.

5.1 Verantwortung für IT Produkte und Dienste

Zurzeit bestimmen die großen Technologiehersteller und Dienste-Anbieter (Marktführer) wie Google, Apple, Samsung, Facebook und Microsoft, was wir als Nutzer für IT-Systeme brauchen (Smartphones, Wearables, …). Doch eine ganzheitliche Verantwortung für ihre IT-Lösungen übernehmen sie nicht. Was wir allerdings dringend benötigen, ist eine Herstellerverantwortung wie in der Automobilbranche! Wenn wir heute ein Auto kaufen, übernimmt der Hersteller, bei dem wir das Auto kaufen, uns gegenüber die volle Verantwortung. Auch die Automobilhersteller arbeiten mit mehreren hundert Zulieferern zusammen. Und doch gibt es für uns immer nur einen Ansprechpartner. Die Hersteller lassen die Autos überprüfen und wenn sie einen Fehler erkennen, werden große Rückrufaktionen gestartet, um Fehler zu beheben, bevor die eigentlichen Probleme auftreten. Dies hat ein sehr großes Vertrauen bezüglich der Sicherheit zu den Herstellern aufgebaut. Wer übernimmt die IT-Sicherheitsverantwortung für IT-Systeme? Am Ende keiner! Wenn die IT-Hersteller beginnen würden, die Gesamtverantwortung der IT-Systeme zu übernehmen, dann würden die heutigen IT-Sicherheitsprobleme deutlich geringer. Alle Softwareprogramme und die Hardware wären besser aufeinander abgestimmt, und Fehler würden einfacher gefunden und behoben.

Hier hat das IT-Sicherheitsgesetz einen ersten Schritt getan und z.B. die Anbieter von Webseiten in die Pflicht genommen, dafür zu sorgen, dass keine Schadsoftware über Webseiten verteilt wird. Dieser Bereich muss und wird sich in den nächsten Jahren international weiter entwickeln müssen.

5.2 Zusammenarbeit bei der Verteidigung der wichtigen IT-Systeme

Die grundsätzlich unsicheren und nicht vertrauenswürdigen IT-Technologien sorgen dafür, dass Angriffe Schaden verursachen. Ist eine Firma Opfer eines Angriffes geworden, versucht diese in der Regel, das Problem alleine und isoliert zu lösen. Die Informationen über erfolgte Angriffe, die Vorgehensweise der Angreifer, den Umfang von Schäden und die Wirkung von Gegenmaßnahmen bleiben somit für die Gesellschaft ungenutzt. Durch eine geordnete und vertrauenswürdige Zusammenarbeit von Firmen und Behörden würde eine deutlich höhere Gesamt-IT-Sicherheit erreicht werden können. Dann wäre z.B. die IT-Sicherheitslage besser einschätzbar, die kritischen Schwachstellen würden gemeinsam identifiziert, die Widerstandsfähigkeit zusammen erhöht, die Verteidigungskosten reduziert und der Zugang zu qualifizierten IT-Sicherheitsexperten gemeinsam optimiert. Aus diesem Grund brauchen wir Modelle, die eine Zusammenarbeit motivieren, damit insgesamt weniger Geld für IT-Sicherheitsmaßnahmen erforderlich wird und ein gemeinsames geringeres Schadensrisiko für alle kooperierenden Organisationen erzielt werden kann.

5.3. Zusammenarbeit mit den IT-Marktführen aus anderen Ländern/Digitale Souveränität

Die wichtigsten IT-Technologien, IT-Produkte und IT-Dienste kommen zurzeit von einigen wenigen IT-Marktführen aus den USA und erfüllen aus sehr unterschiedlichen Gründen unsere Ansprüche an IT-Sicherheit und Datenschutz nicht.

Digitale Souveränität beschreibt die Fähigkeit, die Vertrauenswürdigkeit, Integrität, Verfügbarkeit der Datenübertragung, -speicherung und -verarbeitung durchgängig kontrollieren zu können. Entsprechend muss bewertet und sichergestellt werden, dass keine technischen Mittel in Technologien vorhanden sind, die unberechtigten Zugriff, Veränderung oder Weiterleitung der Daten zulassen.

Digitale Souveränität kann durch Kombination vertrauenswürdiger Sicherheitskomponenten mit Drittkomponenten und durch die verlässliche Evaluierung der verwendeten kritischen Komponenten erreicht werden.

Digitale Souveränität bemisst sich durch den Grad der Selbstbestimmtheit und Kontrolle über die jeweiligen Glieder der Datenkette: Erhebung, Übertragung, Verarbeitung und Speicherung [4].

IT Security Replaceability
Bei der IT Security Replaceability stellen die IT-Markführer offene Schnittstellen zur Verfügung, die eine Austauschbarkeit von IT-Sicherheitstechnologien einfach und nachhaltig in den IT-Produkten und -Lösungen möglich macht. Hierdurch soll es die Möglichkeit geben, die Schlüsselkomponenten und Sicherheitsanker bestehender Produkte gegen vertrauenswürdige IT-Sicherheitstechnologien aus Deutschland und Europa austauschen zu können.

Echte Souveränität durch eigenen Technologie
Wir haben die einmalige Chance, die bekannten Fehler und Herausforderungen im Umfeld von „Industrie 4.0" zu meistern. Die zahlreichen Angriffsszenarien und Gefahren sind Motivation genug, um die Kosten und Mühen auf sich zu nehmen. Zusammen mit unserem starken Mittelstand haben wir die Möglichkeit, eine digitale Souveränität aus Deutschland heraus zu entwickeln. Diese digitale Souveränität ist nicht nur auf „Industrie 4.0" begrenzt, denn viele Ergebnisse werden sich ebenfalls positiv auf das gesamte Internet auswirken. Das was Deutschland bisher im Internet verpasst hat, könnte mit Blick auf unsere gute Positionierung im Umfeld der Industrie wieder wettgemacht werden.

6. Einordnung

Heute werden die unterschiedlichen Aktivitäten im Bereich der IT-Sicherheit für unterschiedliche Sichtweisen betrachtet und IT-Sicherheitsmaßnahmen für die IT-Sicherheitskultur mit unterschiedlicher Reichweite diskutiert und umgesetzt.

Im Rahmen der EU werden zunehmend mit Hilfe von Richtlinien und Verordnungen auf der europäischen Ebene die Wertvorstellungen bezüglich Datenschutz und Vertrauensdienste (eIDAS) etabliert und dadurch in der EU vereinheitlicht.

Im Bereich des Schutzes der kritischen Infrastrukturen wird durch das IT-Sicherheitsgesetz insbesondere die deutsche Gesellschaft bezüglich Cyber War adressiert.

Was wir im globalen Internet auf jeden Fall benötigen ist eine gemeinsame internationale IT-Sicherheitskultur. Leider wollen die unterschiedlichen Länder noch zu stark ihren individuellen Einfluss gelten machen. Dabei ist es besonders wichtig, dass die internationalen IT-Marktführer, die Wertvorstellungen aller Internet-Nutzer weltweit berücksichtigen. Dazu müssen sich die Internet-Nutzer global austauschen, um dieses Ziel gemeinsam zu erreichen.

6.1 Angemessener Risikolevel

Eine spannende Frage ist, was eine angemessene IT-Sicherheit ist, oder welches Risiko an möglichen Schäden wir uns an Gesellschaft leisten können.

Im IT-Sicherheitsgesetz wird vom Stand der Technik gesprochen. Der „Stand der Technik" kann mittel und langfristig helfen, auf ein angemessenes Risikolevel für unsere Gesellschaft zu kommen. Voraussetzung ist, dass alle Organisationen und Institutionen ihre IT-Systeme mit dem Stand der Technik im Bereich der IT-Sicherheit schützen. Was sollte der Stand der Technik bedeuten?

Die IT-Sicherheitsmaßnahmen sind grundsätzlich in der Lage, gegen aktuelle wichtige Bedrohungs- und Angriffsszenarien angemessen zu wirken. Die Hersteller/Anbieter der IT-Sicherheitsmaßnahmen stellen Technologien, Produkte und Dienste zur Verfügung, die bezahlbar und benutzbar sind. Diese IT-Sicherheitsaspekte sollen prinzipiell auch durch vertrauenswürdige Instanzen überprüft werden.

6.2 IT-Sicherheitsgesetz – Regulierte Sicherheitskultur?

Die Voraussetzungen in Deutschland bezüglich wichtiger und verfügbarer IT-Sicherheitstechnologien sind sehr gut, die Konzepte der Kooperationen mit den wichtigen IT-Marktführen und den Peergruppen sind vorhanden und eine gute Basis einer IT-Sicherheitskultur ist vorhanden.

Das IT-Sicherheitsgesetz sorgt dafür, dass das Thema IT-Sicherheit einen angemessenen Stellenwert in unserer modernen Internet-Gesellschaft erhält und stellt den Rahmen für eine vertrauensvolle Kooperation bereit, damit sich eine passende IT-Sicherheitskultur in unserer sich verändernden modernen Gesellschaft entwickelt.

7 Zusammenfassung

Wenn wir die positiven Möglichkeiten der modernen IT und des Internets strategisch nutzen wollen, dann müssen wir sehr kurzfristig neue Wege einschlagen, um zukünftig damit sicher und vertrauenswürdig arbeiten zu können.

Das IT-Sicherheitsgesetz stellt für Deutschland einen notwendigen Rahmen bereit, um sich gegen Cyber War schützen zu können. Auf der Ebene der EU werden der Datenschutz und die Vertrauensdienste behandelt, um mehr Vertrauenswürdigkeit erreichen zu können. Mittel und langfristig müssen wir aber noch Prozesse anstoßen, die eine globale und gemeinsame IT-Sicherheitskulturentwicklung möglich macht. Hier sind auch neue Konzepte und Denkweisen für die Zukunft wünschenswert und langfristig notwendig: Open Data als großes Gewicht für eine offene digitale Gesellschaft und der Faktor Open Source für mehr Transparenz und Verantwortungsbewusstsein müssen zukünftig stärker thematisiert und diskutiert werden. Des Weiteren muss ebenfalls der Faktor Mensch bei jedem dieser Schritte berücksichtigt werden, denn nur eine entsprechende Sensibilisierung und ein ausgeprägtes Verständnis für das Thema erlauben es, die richtigen Entscheidungen zur richtigen Zeit zu treffen.

Eine moderne Gesellschaft sollte diese notwendigen Schritte für das Erreichen einer passenden IT-Sicherheitskultur gemeinsam und zügig für die Sicherung der Zukunft umsetzen.

Literatur

[1] Anzahl der Internetnutzer und Gesamtbevölkerung in Deutschland im Juli 2015 (in Millionen), Quelle: Statista. http://de.statista.com/statistik/daten/studie/151619/umfrage/anzahl-der-internetnutzer-in-den-letzten-drei-monaten-und-gesamtbevoelkerung-in-deutschland/

[2] N. Pohlmann: „Cyber Security", WISU – Das Wirtschaftsstudium, Lange Verlag, 2/2015

[3] R. Fritzen, N. Pohlmann: „Von überall her – Internetdienste vor DDoS-Angriffen schützen", iX – Magazin für professionelle Informationstechnik, Heise-Verlag, 09/2015

[4] G. Niessen, N. Pohlmann: „Der Aufschwung der Vertrauensdienste!? Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt – eIDAS", IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 4/2015

[5] http://www.zvei.org/Verband/Publikationen/Seiten/Staerkung-Vertrauenswuerdiger-IT-Infrastrukturen.aspx