DAS MANIFEST ZUR IT-SICHERHEIT

Erklärung von Zielen und Absichten zur Erreichung einer angemessenen Risikolage in der IT

Herausgeber:
VOICE-Bundesverband der IT-Anwender e.V.
TeleTrusT-Bundesverband IT-Sicherheit e.V.

Der Level an IT-Sicherheit und Vertrauenswürdigkeit ist in Deutschland zurzeit nicht ausreichend. Es gibt keine Perimeter mehr und es fehlt allgemein an Wissen, Verständnis, Einschätzungskompetenz, Technologien und Vorgehensweisen.
Viele IT-Produkte erreichen nicht den nötigen Reifegrad in den Aspekten der IT-Sicherheit, um ein grundlegendes Maß an Vertrauenswürdigkeit zu gewährleisten.
Die IT-Sicherheitstechnologien aus Deutschland sollten breitflächiger und stärker zum Einsatz gebracht werden, um weniger Risiko in den IT-Sicherheitsproblemfeldern Wirtschaftsspionage sowie Cyber-War und Cyber-Sabotage zu erzielen. Dazu wurden die IT-Sicherheitsproblemfelder und wichtigen Aufgaben in diesem Manifest zusammengetragen.

Dieses Manifest ist eine öffentliche Erklärung von **VOICE - Bundesverband der IT-Anwender e.V.** und dem **TeleTrusT - Bundesverband IT-Sicherheit e.V.** zu Zielen und Absichten zur Erreichung einer angemessenen Risikolage in der IT.

Hierfür wurden sechs gemeinsame Thesen erarbeitet, die jeweils spezifische „Gemeinsame Aufgaben“ innerhalb jeder These skizzieren, wie vorhandene Herausforderungen erfolgreich bewältigt werden können.

Für ein höheres Maß an IT-Sicherheit und Vertrauenswürdigkeit. Gemeinsam.

TeleTrusT – Bundesverband IT-Sicherheit e.V.
VOICE - Bundesverband der IT-Anwender e.V.

1. These

Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung!

Die IT hat mit immensen Sicherheitsproblemen zu kämpfen –
werden diese in der Zukunft nicht beseitigt, ist eine nachhaltige Digitalisierung nicht möglich.

IT ist „der Motor“ und die Basis für das Wohlergehen unserer modernen und globalen Informations- und Wissensgesellschaft. Wir müssen feststellen, dass seit Beginn der IT die IT-Sicherheitsprobleme jedes Jahr größer und nicht kleiner werden. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer Endgeräte, Server und Netzkomponenten nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten.

Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zu Nutze machen, Malware installieren, Passwörter sowie Identitäten stehlen und unsere Endgeräte ausspionieren. Ungesicherte IT-Systeme genießen zu viel Toleranz bei Nutzern und Unternehmen. Diese Einstellung wird sich in Zukunft mit der Bedeutung der IT in unserer Gesellschaft radikal ändern müssen.

Eine angemessene, sichere und vertrauenswürdige IT gemeinsam zu bewältigen, ist für die erfolgreiche Zukunft unserer Informations- und Wissensgesellschaft entscheidend. Letztlich muss die angestrebte Digitalisierung auch die Nachhaltigkeit als strategisches Ziel haben. Das gelingt nur, wenn die IT-Technologien und -Services sicher und vertrauenswürdig sind.

Gemeinsame Aufgaben

Die Gesellschaft muss intolerant gegenüber unsicheren IT-Lösungen sein!

Alle Interessengruppen müssen für eine erfolgreiche und nachhaltige Umsetzung einer gemeinsamen sicheren und vertrauenswürdigen IT bessere und wirkungsvollere IT-Lösungen entwickeln und einsetzen. Dies erfordert eine genaue Spezifikation der Wünsche der Anwender und die Bereitschaft, diese durch die von IT-Herstellern bereitgestellten sicheren und vertrauenswürdigen IT-Lösungen auch einzusetzen.

In der Zukunft werden wir risikobasierte Ansätze und adaptive IT-Sicherheits-Architekturen sowohl in den primären Applikationen als auch in den industriellen Steuerungskomponenten (Maschinen und Anlagen) realisieren und nutzen. Der immer schneller werdende Digitalisierungsprozess setzt voraus, den Aspekt der IT-Sicherheit in neuen IT-Architekturen, IT-Anwendungen und industriellen Steuerungskomponenten umzusetzen. Für die erfolgreiche Erreichung dieses Ziels ist es notwendig, sowohl Informationstechnologie (IT) als auch Operational Technology (OT) zu betrachten und die Schnittstellen gemeinsam zu standardisieren. IT-Sicherheit ist kein Business-Enabler mehr, sondern eine wichtige Grundanforderung im End-to-End Prozess.

In den IT-Technologien sowie den IT-Sicherheitsanforderungen muss zwischen kommunikativer Digitalisierung und industrieller Digitalisierung differenziert, aber eine gemeinsame IT-Sicherheitsstrategie berücksichtigt werden.

Ein wichtiges Alleinstellungsmerkmal in nationaler Hinsicht ist der Aspekt der qualitativen IT-Sicherheit. „IT Security made in Germany“ hat sich bereits als Aushängeschild für deutsche IT-Sicherheit und Datenschutz etabliert. Die Schaffung und Förderung der IT-Sicherheitssouveränität ist hingegen noch eine wichtige Herausforderung, die bewältigt werden muss.

Hard- und Software-Schwachstellen müssen von den Herstellern schnellstmöglich geschlossen werden. Anwender sind in der Pflicht, diese Nachbesserungsmöglichkeiten unverzüglich wahrzunehmen. Bekanntermaßen erfolgt ein Großteil erfolgreicher Angriffe über veraltete Software. Bekannte Konzepte, auf denen die heutige Softwareentwicklung aufsetzt, müssen im Hinblick auf IT-Sicherheitsaspekte überprüft, und gegebenenfalls neu entworfen werden. Das Sicherheitsniveau eines IT-Produktes muss klar erkennbar, überprüfbar und mit anderen vergleichbar sein.
Auch die Hardware-nahen IT-Lösungen, wie z.B. im Internet of Things - IoT, brauchen innovative Konzepte, wie Schwachstellen schnell und einfach gepatcht werden können. Hersteller, Integratoren, Betreiber und Anwender von IT-Sicherheitslösungen müssen ihre Verantwortung stärker wahrnehmen.

2. These

Gemeinsam mehr wirkungsvollere IT-Sicherheitslösungen nutzen!

Stark fragmentierte Sicherheitsprodukte und ein fehlendes gemeinsames Vorgehen machen es für Unternehmen schwer, die passenden sicheren und vertrauenswürdigen IT-Lösungen zu finden und einzusetzen.

Die Angriffsflächen der IT-Technologie werden durch komplexere Software und kompliziertere Zusammenhänge zwischen Protokollen, Diensten, IT-Geräten und globalen Infrastrukturen vielfältiger und deutlich größer. Bei einer nachhaltigen Digitalisierung brauchen wir umfangreiche und übergreifende IT-Konzepte. Harmlose Geräte wie z.B. Kaffeemaschinen, Drucker, Smart-watches etc. werden bereits heute erfolgreich als Einfallstor für Angriffe missbraucht.

Es gibt zahlreiche vorhandene IT-Sicherheitstechnologien, die helfen könnten, deutlich weniger Risiko zu erzielen und damit Schäden zu reduzieren, wenn sie flächendeckend eingesetzt würden. Gründe, die dafür sorgen, dass nicht mehr wirkungsvolle IT-Sicherheitslösungen eingesetzt werden, sind z.B.:

- Schlechte Bedienbarkeit der IT-Sicherheitslösungen
- Zu viele unterschiedliche Produkte, die zusammenarbeiten und verwaltet werden müssen
- Kein Vertrauen in die Wirkung der IT-Sicherheitslösungen
- Probleme bei der Integration von IT-Sicherheitstechnologien in Standardlösungen
- Fehlender internationaler Support

Die heutigen IT-Sicherheitsprodukte sind stark fragmentiert. Kleinere Anbieter decken nur Nischen ab. Dies bedeutet, dass für den breiten Schutz gegen diverse Bedrohungen zahlreiche kleine Nischenlösungen „übereinander gestapelt“ zum Einsatz kommen müssen. Dies ist auf Dauer nicht nur inakzeptabel, sondern auch sehr ineffizient. Eine „Komplettlösung“ aus einer Hand eines nationalen Herstellers existiert in Deutschland nicht.

Ein Unternehmen allein für sich hat es schwer, etwas zu bewegen. Erst wenn alle beteiligten Interessengruppen eng zusammenarbeiten, können wir einen höheren und angemessenen Level an Sicherheit und Vertrauenswürdigkeit in der IT erreichen und damit das Risiko auf ein angemessenes Maß reduzieren. Ein vertretbares IT-Sicherheitsrisiko kann die Digitalisierung beflügeln und die Nachhaltigkeit möglich machen. Ohne eine gemeinsame Umsetzung einer festgelegten IT-Sicherheitsstrategie wird eine erfolgreiche nachhaltige Digitalisierung in Deutschland scheitern.

Gemeinsame Aufgaben

Gemeinsam für mehr wirkungsvolle IT-Sicherheit in unseren IT-Lösungen!

Ein umfangreiches und übergreifendes IT-Konzept muss erstellt werden, damit ein nachhaltiger Digitalisierungsprozess möglich ist und alle IT-Komponenten ins Risikomanagement einfließen können. Die Standardisierung von Schnittstellen für die Zusammenarbeit von IT-Lösungen verschiedener Hersteller und unterschiedlicher Anwender muss gemeinsam umgesetzt werden.

Wir müssen vom angebotsgetriebenen zum anforderungsgetriebenen IT-Sicherheitsmarkt kommen. Dazu sollten die Anwenderunternehmen gemeinsam ihre Einkaufsmacht fair nutzen. Eine enge Zusammenarbeit zwischen den Herstellern und Anwendern ist nötig, um angemessene, wirkungsvolle, sichere und vertrauenswürdige IT-Lösungen in den operativen Einsatz zu bringen und umfangreiche und übergreifende IT-Konzepte erfolgreich umzusetzen.

Die Zusammenarbeit mit IT-Marktführern ist notwendig, um eine optimale Integration von IT-Sicherheitslösungen in Hard- und Software umsetzen und überprüfen zu können. Es müssen gemeinsame IT-Kompetenzzentren aufgebaut werden, um gemeinsame Synergieeffekte erzielen zu können.

Die Erarbeitung und Festlegung einer gemeinsamen IT-Sicherheitsstrategie mit konkreten Zielen wie der Sicherheit und Vertrauenswürdigkeit in der IT, die gemeinsam mit allen Interessengruppen erreicht werden kann, ist notwendig. Gemeinsame wichtige Ziele genießen eine hohe Priorität, weshalb über die kleinste gemeinsame Schnittmenge hinausgegangen werden muss.

Am Ende ist eine nachhaltige Umsetzung der IT-Sicherheitsstrategie mit allen Interessengruppen notwendig.

3. These

Verschlüsselung, Transparenz und Vertrauen sind die digitalen Werkzeuge für die informationelle Selbstbestimmung!

Um sichere IT-Produkte verlässlich nutzbar zu machen, sind Transparenz und Vertrauen nötig.

Damit IT-Technologien und IT-Dienste in unserer Gesellschaft positiv genutzt werden, müssen sie sicher und vertrauenswürdig sein. Verschlüsselung ist ein besonders wirkungsvoller und notwendiger IT-Sicherheitsmechanismus. Potenzielle Angriffsflächen werden reduziert und digitale Werte werden angemessen geschützt. Das trifft auf die Privatsphäre aller Bürger, genauso wie für den Schutz von Unternehmenswerten zu. Wir brauchen flächendeckende Verschlüsselung für die Übertragung und Speicherung digitaler Informationen. Dazu brauchen wir sichere und vertrauenswürdige Verschlüsselungsprodukte, die einfach zu integrieren und zu nutzen sind.

Insbesondere im Bereich der Kommunikationsverschlüsselung ist eine einfache Einführung möglich und sollte gemeinsam umgesetzt werden. Bei der Verschlüsselung von gespeicherten digitalen Werten müssen die passenden IT-Sicherheitsinfrastrukturen bereitgestellt werden, damit die Bedürfnisse der Unternehmen bezüglich der Verfügbarkeit gewährleistet werden. Der Schutz des geistigen Eigentums unserer Gesellschaft muss in Zukunft mit Hilfe von Verschlüsselungs-systemen sichergestellt werden.

Die staatlich motivierten Schwachstellen und Hintertüren sorgen für weniger Sicherheit und zerstören das Vertrauen in die immer wichtiger werdenden IT-Technologien und IT-Dienste.

Für den nachhaltigen Digitalisierungsprozess ist es wichtiger, die digitalen Werte in der Informations- und Wissensgesellschaft zu schützen, als potentielle Zugriffe von Geheimdiensten und Strafverfolgungsbehörden durch eine generelle Schwächung von IT-Lösungen zu ermöglichen.
Sobald IT-Produkte bereits „unsicher“ am Markt veröffentlicht oder IT-Sicherheitsfeatures erst auf Nachfrage des Benutzers angeboten werden oder zu- bzw. abschaltbar sind, wird der Sinn und Zweck von IT-Sicherheit ausgehebelt. Das muss vermieden werden.

Gemeinsame Aufgaben

Um digitale Werte umfänglich zu schützen, müssen sie sicher verschlüsselt werden!
Transparenz und Vertrauen müssen vom Alleinstellungsmerkmal zum Standard-Ausstattungsmerkmal eines IT-Produktes werden!

Die Hersteller und Anwender von Verschlüsselungslösungen werden enger zusammenarbeiten, damit nicht nur mehr Verschlüsselung zum aktiven Einsatz kommt, sondern auch eine bessere Bedienbarkeit, eine einfachere Integration und ein besseres Management möglich gemacht werden. Zukünftige Verschlüsselungsprodukte müssen, ähnlich wie der Airbag im Auto, sicher und vertrauenswürdig, aber für den Nutzer möglichst transparent sein.

Post-Quanten-Kryptografie ist im Hinblick auf die Zukunft bereits heute ein wichtiger Aspekt und muss entsprechend berücksichtigt werden. Gemeinsam werden wir vorhandene Hemmnisse abbauen, damit deutlich mehr Verschlüsselungslösungen zum Einsatz kommen.

Wir werden nur IT-Technologien und -Dienste erstellen und nutzen, die keine staatlich motivierten Schwachstellen und Hintertüren in IT-Lösungen beinhalten. Die EU-Länder und die EU sollen sich klar für den Schutz der digitalen Werte positionieren und dafür sorgen, dass mehr sichere und vertrauenswürdige IT-Technologien und IT-Dienste entwickelt und genutzt werden.

Deutschland darf nicht, durch gesetzliche Verpflichtungen oder auf anderen Wegen, die Schwächung von IT-Technologien veranlassen. Dies würde die Wirkung von IT-Sicherheit beschädigen und damit die Privatsphäre aller Bürger, wie auch Unternehmenswerte in Gefahr bringen und den Erfolg der digitalen Transformation ausbremsen.

Anwender und Hersteller erteilen einer staatlich motivierten Schwächung von Kryptografie oder den Wünschen nach Hintertüren gemeinsam eine Absage.

Vertrauen und Transparenz werden bei der Bewertung und Auswahl von IT-Lösungen eine besondere Rolle spielen.

4. These

Security-by-Design, Privacy-by-Design und nachvollziehbare Qualitätssicherung sind unabdingbar!

Die Entwicklungsparadigmen Security-by-Design sowie Privacy-by-Design und nachvollziehbare Qualitätssicherung müssen für alle IT-Lösungen bedingungslos umgesetzt werden, um mehr Sicherheit und Vertrauenswürdigkeit zu erzielen.

Transparenz ist ein wichtiger Aspekt von Vertrauen. Offene Systeme, IT-Architekturen und IT-Produkte erlauben es, bei Bedarf Sicherheit und Vertrauenswürdigkeit zu überprüfen. Ein Großteil unserer Gesellschaft funktioniert mit und dank Open Source Software. Die Qualität und die Prozesse rund um die Entwicklung der quelloffenen Software bergen großes Verbesserungspotential bezüglich Sicherheit und Vertrauen in die IT. Das Verbesserungspotential für sichere und vertrauenswürdigere Software, insbesondere Open Source Software, muss gemeinsam erfolgreich gefördert, gefordert und genutzt werden.

IT-Sicherheit, die direkt im Design und bei der Entwicklung von Software sowie Hardware berücksichtigt wird, ist deutlich wirkungsvoller und einfacher in der Bedienung. Dies sorgt für eine breitere Nutzerakzeptanz und einen höheren Verbreitungsgrad, was dann wiederum für ein höheres Maß an IT-Sicherheit und Vertrauenswürdigkeit in der IT sorgt.

Gemeinsame Aufgaben

Security-by-Design und Privacy-by-Design Software vermeiden hohe nachträgliche Sicherheitsassessments, weshalb zukünftige Vorhaben diese Anforderungen erfüllen müssen, während bereits Open Source Software, welche millionenfach im Einsatz ist, bezüglich der IT-Sicherheitsaspekte nachhaltig überprüft werden muss!

Eine (Mit)Verantwortung aller Nutzer für wichtige Open Source-Komponenten muss übernommen werden. Der gemeinsame Aufbau eines Fonds, um finanzielle Mittel für die Verbesserung der Softwarequalität von wichtigen Open Source-Komponenten zur Verfügung zu stellen, ist nötig. Neben der Durchführung regelmäßiger Sicherheitsassessments weit verbreiteter und gemeinsam genutzter Software, sollte die Formulierung und Förderung von wünschenswerten, gemeinsam nutzbaren Open Source Technologien möglich sein.

Security-by-Design und Privacy-by-Design sind wichtige Entwicklungsparadigmen bei der Herstellung, Bewertung und Auswahl von IT-Lösungen.

Alle Akteure werden helfen, durch den immer schneller werdenden Digitalisierungsprozess moderne sichere und vertrauenswürdige IT-Technologien schnell in die Fläche von wichtigen und zukunftsorientierten Anwendungsbereichen zu bekommen.

Die Benutzbarkeit und Nutzererfahrung von IT ist das Allesentscheidende und muss vom Nutzer aus betrachtet werden. Die entwickelte Software, welche von externen Unternehmen oder internen Abteilungen stammt, muss Security-by-Design und Privacy-by-Design in der Zukunft einen höheren besonderen Stellenwert zuordnen.

5. These

Wir brauchen eigene Souveränität von IT-Sicherheitsinfrastrukturen!

Europa mangelt es an einer eigenen IT-Sicherheitsinfrastruktur – für eine eigene Souveränität und sichere und vertrauenswürdige IT-Lösungen ist sie unerlässlich.

IT-Sicherheitsinfrastrukturen wie z.B. für VPNs, E-Mail-Verschlüsselung, elektronische Identitäten, Domänenzertifikate usw. sollten hinsichtlich der Herkunft von Technologien und Produkten in europäischer Verantwortung liegen.

Das vorherrschende Ziel ist es, die eigene Souveränität von IT-Sicherheitsinfrastrukturen zu bewahren und – falls notwendig – wiederzuerlangen. Die digitale Souveränität ist ein essentiell wichtiger Baustein für die digitale Selbstbestimmung – insbesondere für die IT-Infrastruktur.

Gemeinsame Aufgaben

Der technologische Stand in Europa muss gesichert, ausgebaut und gefördert werden, um die eigene Souveränität für wichtige IT-Infrastrukturen sicherzustellen!

Die EU muss kurz- bis mittelfristige Maßnahmen ergreifen, um die Souveränität im Bereich IT-Sicherheit aufzubauen und zu sichern.

Bei den eingesetzten IT-Lösungen muss dem Attribut „IT-Sicherheitsinfrastruktur in Europa“ ein besonderer Wert zugemessen werden. Nur so kann eine selbstbestimmte Handlung der Unternehmen und unserer ganzen Gesellschaft sichergestellt werden.

Aufsichtsräte und Beiräte von deutschen/europäischen Unternehmen müssen in ihren Strategien die Anforderungen an IT-Sicherheit sowohl für Produkte als auch für Dienstleistungen und Anwendungen hinterfragen und bewerten.

6. These

Cyber-War, Cyber-Sabotage und Cyber-Spionage werden immer bedrohlicher!

Ein erfolgreicher Angriff auf die kritischen Infrastrukturen ist ein sehr großes Risiko für die meisten Unternehmen.

Cyber-War, Cyber-Sabotage und Cyber-Spionage durch andere Staaten oder terroristische Gruppen stellen eine neue Gefahr dar, die das Risiko für unsere Gesellschaft und die einzelnen Unternehmen deutlich verändert und steigert.

Mit der Hilfe von Cyber-Angriffen werden politische Ziele einfacher und preisgünstiger umgesetzt. Das Beispiel STUXNET zeigt, wie Staaten mit einer intelligenten Malware in der Lage waren, durch Cyber-Sabotage die Uran-Aufbereitung in einem speziellen Land um zwei Jahre zu verzögern.

Aus diesem Grund werden auch Anwendungen, die heute als sicher gelten, neu beurteilt werden müssen. IT-Konzepte, Richtlinien und Schulungen sind nötig, um nicht nur den technischen Aspekt abzusichern.

Gemeinsame Aufgaben

Bietet eine IT-Lösung das Potenzial, negative Auswirkung auf die kritischen Infrastrukturen auszuüben, so muss sie besonders sorgfältig geprüft und regelmäßig kontrolliert werden!

Alle wichtigen IT-Anwendungen werden unter dem Aspekt Cyber-War, Cyber-Sabotage und Cyber-Spionage beleuchtet und neu bewertet, damit IT-Sicherheitsmaßnahmen für einen angemessenen sicheren und robusteren Betrieb umgesetzt werden können.

Die immer wichtiger werdende Bedrohung Cyber-Angriff wird in die Risikobewertung der Unternehmen eingebunden. Eine Zusammenarbeit aller Interessengruppen, unabhängig von gesetzlichen Verpflichtungen, soll zum Erreichen einer höheren Sicherheit und Robustheit umgesetzt werden.

Um große gesellschaftliche Schäden zu verhindern, muss jedoch auch in Prävention, Detektion und Reaktion investiert werden. Notfallpläne für ein Worst-Case Szenario sind ebenso nötig, wie die Entwicklung von Krisenstabsübungen und die Bildung von Eingreiftruppen.

Workshop "Digital Security"

Die Grundlagen für „Das Manifest zur IT-Sicherheit“ wurden im Workshop „Digitale Security“ im Rahmen des „VOICE ENTSCHEIDERFORUM: Innovation meets Operational Excellence: IT Applied” in Wien im September 2016 diskutiert und entwickelt.

Moderatoren des Workshops waren:

Prof. Dr. Norbert Pohlmann, Leiter des Instituts für Internet-Sicherheit - if(is) und Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V.

Dr. Rolf Reinema, Head of Technology Field IT-Security, Siemens AG

Teilnehmer des Workshops waren:

Sebastian Barchnicki, Unternehmensstrategie & Alliance Management, secunet Security Networks AG

Uwe Beikirch, Vorstand, baramundi software AG

Rainer Göttmann, CEO, metafinanz Informationssysteme GmbH

Prof. Dr. Udo Helmbrecht, Geschäftsführender Direktor, ENISA - European Union Agency for Network and Information Security

Dr. Andreas Huth, Vorstand, Beta Systems Software AG

Detlef Henze, Konzernbereichsleiter IT, TÜV Austria Holding AG

Wolfram Müller, IT-Leiter, EUROGATE GmbH & Co. KGaA

Patrick Quellmalz, Leiter Services, VOICE - Bundesverband der IT-Anwender e.V.

Stepan Seycek, Doktorand, Universität Wien

Ansprechpartner

Prof. Dr. Norbert Pohlmann

Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrust e.V.

Institut für Internet-Sicherheit – if(is)

Westfälische Hochschule Fachbereich Informatik & Kommunikation

Neidenburger Str. 43

45897 Gelsenkirchen

Fon (+49) (0)209 / 9596-515

Mobil (+49) (0)173 / 3021 838

Mail pohlmann@internet-sicherheit.de

Sebastian Barchnicki

Unternehmensstrategie & Alliance Management

secunet Security Networks AG

Kurfürstenstr. 58

45138 Essen

Fon (+49) (0)201 / 5454-1013

Mail sebastian.barchnicki@secunet.com

Patrick Quellmalz

Leiter Services

VOICE - Bundesverband der IT-Anwender e.V.

Büro Köln: Haus 1, Waltherstraße 49-51, 51069 Köln

Fon (+49) (0)30 / 2084 964 73

Mobil (+49) (0)176 / 84 36 57 36

Mail patrick.quellmalz@voice-ev.org

Glossar

Hintertür

Mithilfe einer Hintertür (Backdoor) erhalten, aus der Sichtweise des Betreibers, unberechtigte Dritte Zugang zum IT-System.

Industrielle Digitalisierung

Die industrielle Digitalisierung ermöglicht die Kontrolle, Steuerung und Analyse von Komponenten im industriellen Umfeld, die zunehmend mit IP-Netzen verbunden sind, z.B. Industrial Internet, Industrie 4.0, usw.

Informationstechnologie (IT)

Das gesamte Spektrum an Technologien zur Datenverarbeitung, wie Software, Hardware, Kommunikationstechnologien und damit verbundene Services.

IT Security made in Germany

Ein IT-Sicherheitsunternehmen muss insgesamt 5 Kriterien für das Qualitätszeichen erfüllen. U.a. wird ein Unternehmenssitz in Deutschland gefordert, keine Hintertüren in Produkten und Services sowie die Einhaltung des deutschen Datenschutzgesetzes. https://www.teletrust.de/itsmig/

IT-Sicherheitssouveränität

IT-Sicherheitssouveränität bedeutet, dass die IT-Lösungen unabhängig von anderen Staaten sicher und vertrauenswürdig realisiert und betreiben werden können. Die IT-Sicherheitssouveränität wird mit der zunehmenden Bedrohung von Cyber-War, Cyber-Sabotage und Cyber-Spionage immer wichtiger.

Kommunikative Digitalisierung

Alle derzeitig digitalen Möglichkeiten, mit anderen Menschen oder Computern in Kontakt zu treten, werden im Allgemeinen als kommunikative Digitalisierung bezeichnet.

Kritische Infrastruktur

Kritische Infrastrukturen sind Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Im Rahmen des Manifests sind insbesondere die IT-Lösungen von Kritische Infrastruktur der Unternehmen gemeint.

Operational Technology (OT)

OT ist Hardware und Software, die eine Änderung durch die direkte Überwachung und/oder Kontrolle von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erkennen oder verursachen (Betriebstechnik).

Interessengruppen

In diesem Manifest werden Interessengruppen als Personengruppen bezeichnet, die das gemeinsame Interesse haben, die IT sicherer und vertrauenswürdiger zu gestalten. Diese kommen aus den Bereichen: Politik, Verwaltung, IT-Sicherheitsforschung, Anwendung und Herstellung (IT-Sicherheitsindustrie).

Herausgeber:

Prof. Dr. Norbert Pohlmann
Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V.
Leiter des Instituts für Internet-Sicherheit – if(is)

Dr. Thomas Endres
Vorsitzender des Präsidiums VOICE - Bundesverband der IT-Anwender e.V.

Berlin, den 15.12.2016