BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitsmanagement

Schätzen mit System

Wie können IT-Sicherheitsteams den Aufwand von Schutzmaßnahmen bemessen? Diese Frage beschäftigt Unternehmen und Behörden immer wieder aufs Neue. Eine Arbeitshilfe zur Planung für Ressourcen in IT-Sicherheitsteams bietet nun eine Lösung und konnte sich in kürzester Zeit bereits als anerkannte Schätzmethode etablieren.

Von Günther Ennen, BSI

Ein erfolgreiches Managementsystem der Informationssicherheit (ISMS) braucht Struktur, Organisation und Personal. Erhebungstechniken für quantifizierbare Aufgaben können für die Ermittlung von Personalbedarf nicht in jedem Fall eingesetzt werden, stattdessen werden überschlägig geschätzte Prognosen vorgenommen. Welche personelle Stärke ist für ein IT-Sicherheitsteam angemessen? Eine Frage, die in der Vergangenheit zu vielen ergebnisoffenen Diskussionen geführt hat.

Ein Schätzverfahren zur Feststellung des Aufwands und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams, bei dem auch der Bundesrechnungshof mitgewirkt hat, ist nun als Lösung und Arbeitshilfe anerkannt. Damit lassen sich Aufgaben zur Informationssicherheit, Prioritätensteuerung und zeitlicher Aufwand transparent darstellen. Das Schätzverfahren beschreibt die fachlichen Anforderungen für ein effektives ISMS und unterstützt dabei, den Mindestpersonalbedarf zu ermitteln.

Möglichkeiten und Grenzen

Empirische Daten zur Berechnung des Aufwands für die Tätigkeiten der IS-Teams liegen nicht vor, daher ist es zulässig und hilfreich, mit Schätzungen zu beginnen. Als Basis hierfür dienen Erfahrungswerte von Behörden aus der Vergangenheit.

Die Arbeitshilfe erhebt dabei keineswegs den Anspruch, zur Begründung von Bedarfsanforderungen für mehr Personal verwendet zu werden. Oft lassen sich durch eine interne Umorganisation des vorhandenen Personals die Aufgaben zur Informationssicherheit bewältigen.

Die Kriterien zur Schätzung des Aufwands sind so gewählt, dass sie grundsätzlich für jede Behörde anwendbar sind. Behördenspezifische, individuelle Besonderheiten werden hierbei nicht abgebildet. Das

Inhalt

Impressum

Redaktion:
Matthias Gärtner (verantwortlich)
E-Mail: matthias.gaertner@bsi.bund.de

Nora Basting
E-Mail: nora.basting@bsi.bund.de

Sebastian Bebel
E-Mail: sebastian.bebel@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit und Presse
Postfach 20 03 63
53133 Bonn

Hausanschrift:
Godesberger Allee 185–189
53175 Bonn

Telefon: +49 228 999582-0
Telefax: +49 228 999582-5455

Web: www.bsi.bund.de
www.bsi-fuer-buerger.de

Das BSI-Forum, Organ des Bundesamtes für Sicherheit in der Informationstechnik in Bonn, ist Bestandteil der <kes> – Die Zeitschrift für Informations-Sicherheit
24. Jahrgang 2016

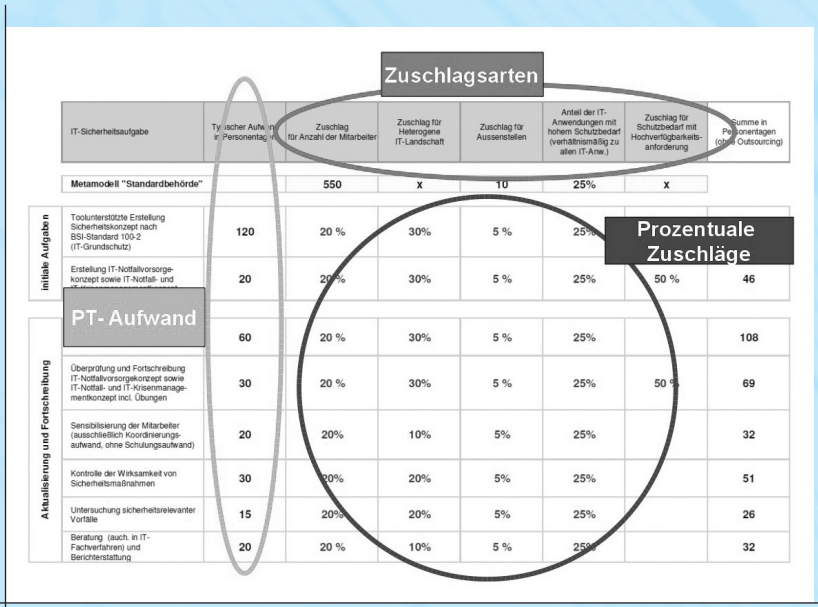

Abbildung 1: Die Arbeitshilfe nutzt als Modell eine Standardbehörde und liefert prozentuale Zuschläge für die Aufwandsabschätzung.

beschriebene Vorgehen entbindet eine Behörde jedoch nicht von der Notwendigkeit, nach einer Konsolidierungsphase zusätzlich eine Personalbedarfsermittlung gemäß den im „Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung“ anerkannten Methoden durchzuführen.

Standardbehörde als Modell

Die Arbeitshilfe geht von dem Modell einer „Standardbehörde“ aus (vgl. Kasten), Abweichungen von dem gewählten „Standard“ werden auf Basis von gewichteten Wertetabellen durch prozentuale Zeitzuschläge beziehungsweise Zeitabschläge hinsichtlich des Aufwands berücksichtigt.

Zu den Aufgaben des ISMS zählen zunehmend die Risikobewertung aktueller Warnungen, die Reaktion auf aktuelle Sicherheitsempfehlungen sowie zeitkritische Warnungen, Hersteller-Sicherheitsupdates und Patches sowie tägliche Berichte zur Lage der Informationssicherheit. Aufgaben, die gemeinhin in Zuständigkeit des IT-Betriebs erfolgen, wie zum Beispiel Tests von Software sowie Abnahme- und Freigabeverfahren, die Mitwirkung bei der Erstellung von Testplänen oder die Bewertung von Sicherheitsprodukten, erfordern ebenfalls die Mitwirkung des Informations-Sicherheits-(IS)-Teams.

Die Arbeitshilfe ist ein minimaler und zielführender Ansatz, der sich in vielen Behörden bereits bewährt hat. Sie wird unter anderem als geeignet angesehen, die Ressourcenplanung der IS-Teams der Bundesländer zu verbessern. Durch die Aufnahme der Arbeitshilfe in das „Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung“ konnte sie sich bereits als Quasi-Standard etablieren.

Die „Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung“ und das Schätztool stehen unter dem folgenden Link kostenlos zum Download bereit: www.bsi.bund.de/Personalschaetzung ■

Die „Standardbehörde“

- _____ hat rund 500 Mitarbeiter
- _____ verfügt über eine homogene IT-Landschaft
- _____ betreibt IT-Systeme und IT-Verfahren mit normalem Schutzbedarf
- _____ hat keine Außenstellen
- _____ benötigt keine Anforderungen an die Hochverfügbarkeit von IT-Systemen oder Anwendungen

Literatur

[1] Bundesministerium des Innern (BMI), Bundesverwaltungsamt (Hrsg.), Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, www.orghandbuch.de

Vertrauen und Informationstechnik

„Trau, schau, wem?" – die „vertrauenswürdige IT", welche als Begriff in viele politische Forderungskataloge und Positionspapiere Einzug gehalten hat, kann nicht unmittelbar entstehen. Sie bedingt nachweislich verlässliche informationstechnische Systeme und vertrauenswürdige Akteure, wie Anbieter und Auditoren. Diese Herleitung basiert auf dem ursprünglichen Konzept von Vertrauen zwischen Menschen und deren Sichtweise auf technisch vermittelte Kommunikation.

Von Dr. Sven Herpig, BSI

Vertrauen ist ein wichtiger Bestandteil des Lebens und seine Abwesenheit kann uns unserer Seelenruhe berauben. Vertrauen kann zu einem ausgeglichenen Lebensgefühl beitragen, hat aber vor allem die Aufgabe, die Komplexität von Entscheidungsprozessen (für Handlungen) drastisch zu reduzieren – auch im Bereich der Informationssicherheit. Eine Wiedergabe des jahrzehntelangen (u. a. soziologischen) Diskurses zu diesem Thema ist an dieser Stelle nicht möglich – aber vielleicht auch gar nicht notwendig.

Vertrauen in Personen und Gesellschaft

Bringt man das Konzept von Vertrauen in Einklang mit der modernen Informationsgesellschaft, kommt es zum Beispiel zu folgender Überlegung: Nehmen wir an, ich bin mit viel Gepäck im Zug unterwegs, tippe gerade an meinem Laptop und möchte kurz ins Bord-Bistro. Ich habe nun mehrere Optionen:

_____ Ich lasse meinen Laptop so wie er ist und gehe los.
_____ Ich sperre meinen Laptop und gehe los.
_____ Ich verhalte mich wie in der vorigen Option, frage aber meinen Sitznachbarn, ob er auf meinen Laptop aufpassen kann.
_____ Ich nehme meinen Laptop mit.

Nun reflektieren genau diese Verhaltensweisen, neben anderen Aspekten, auch eine bestimmte Einstellung zum Thema Vertrauen. In den ersten beiden Fällen kann man problemlos von einem blinden Vertrauen in die eigene Umwelt sprechen – oder von Ignoranz. Der Grat ist sehr schmal – vielleicht hat man die Hoffnung, dass man irgendeiner Person im Blickfeld so weit vertrauen kann, dass diese einen Diebstahl melden würde. Die dritte Verhaltensweise suggeriert eine Beschäftigung mit dem Sitznachbarn und eine Abwägung, ob er oder sie des Vertrauens würdig (lies: vertrauenswürdig) scheint. Die vierte Verhaltensweise deutet auf das Fehlen eines ausreichenden Vertrauens in die Umwelt hin.

Wann stufen wir jemanden als vertrauenswürdig ein? Einen starken Einfluss hat die Sozialisierung, sprich: wie man von Kindheit an gelernt hat zu vertrauen. Dazu kommen dann konkrete (gemeinsame Vergangenheit) oder allgemeine (vergangene Erfahrungen) Erfahrungswerte getreu dem Motto: „fool me once, shame on you – fool me twice, shame on me".

Natürlich spielen viele weitere Faktoren eine Rolle, zum Beispiel ob ich jemandem mein Leben anvertraue oder nur meinen gesperrten, vollverschlüsselten Laptop, von dessen Daten ich zwei Backups besitze.

Im Endeffekt läuft es auf einen zweiteiligen Prozess hinaus:

_____ Prüfung (Kann ich jemandem vertrauen?) und
_____ Risikoabwägung (Was passiert im schlimmsten Fall und welche anderen Möglichkeiten habe ich?)

Dies findet, mit dem Zwischenschritt der Evaluierung, so auch in der Informationssicherheit Anwendung, aber dazu später.

Vertrauen in technisch vermittelte Kommunikation

Bevor man allerdings von dem Vertrauen in Personen auf Vertrauen in informationstechnische Systeme schließt, sollte man den Zwischenschritt über die Kommunikation gehen. Hierbei geht es nicht darum, wie Vertrauen durch Kommunikation entsteht, sondern wie sich Vertrauen in Kommunikation zusammensetzt.

Warum ist das relevant? Wenn ich kein Vertrauen in eine Kommunikation habe, führe ich sie nicht, oder zumindest nicht so, wie ich sie gerne führen würde, wenn ich Vertrauen in die Kommunikation hätte. Das ist wichtig für diejenigen, die Lösungen für technisch vermittelte Kommunikation bereitstellen. Vertrauen die (potenziellen) Nutzer nicht in die Art der technisch vermittelten Kommunikation, werden sie diese nicht kaufen oder nutzen. Das ist schlecht für den Anbieter.

Als Definition lässt sich festhalten: Vertrauen in einen technisch vermittelten Kommunikationsvorgang

besteht, wenn folgende Bedingungen gegeben sind: Anonymität, Geheimhaltung und Willensfreiheit. Die Anonymität bezieht sich natürlich nicht auf das Unwissen, mit wem man gerade kommuniziert, sondern darauf, dass kein Akteur zu etwas anderem als den notwendigen technischen Zwecken diese Kommunikationsbeziehung (lies: Metadaten) temporär aufzeichnet.

Der zweite Punkt geht damit einher: Er erweitert die Verschwiegenheit über die beteiligten Gesprächspartner auf deren Gesprächsinhalte. Da für die Aufzeichnung der beteiligten Gesprächsinhalte keine technische Notwendigkeit besteht, fällt diese sogar komplett weg. Die Willensfreiheit bezeichnet einen Zustand, in dem ich mich nicht durch die Angst vor Überwachung bewusst oder unbewusst selbst zensiere.

Können die drei genannten Punkte in einer technisch vermittelten Kommunikation positiv beschieden werden, so habe ich Vertrauen in die Kommunikation und nutze entsprechende technische Produkte und Systeme – sofern es diese gibt. Edward Snowden hat hierzu folgendes gesagt: „The conversation [Anmerkung: Umgang mit den Inhalten der veröffentlichten Dokumente zur NSA-Spionageaffäre] occurring today will determine the amount of trust we can place both in the technology that surrounds us and the government that regulates it." [1]

Verlass auf informationstechnische Systeme

Bevor beschrieben werden kann, wie Vertrauen in informationstechnische Systeme entsteht, ein kurzer Einwand: sozialwissenschaftlich betrachtet existiert Vertrauen in informationstechnische Systeme nicht – der Anwender kann dem Anbieter vertrauen, also denjenigen Personen, die diese informationstechnischen Systeme hergestellt/bereitgestellt haben und/oder kontrollieren, aber er vertraut nicht den Systemen selbst.

Systeme funktionieren also maximal als Vertrauensintermediäre – durch ihr korrektes Funktionieren vertraut man dem Anbieter. Man verlässt sich darauf, dass diese Systeme so funktionieren wie sie sollen – und wie einem vermittelt wurde, dass sie funktionieren würden. Es wäre daher also eher angeraten, von Verlass auf informationstechnische Systeme zu sprechen.

Damit ist dieser Komplex aber noch nicht ganz abgeschlossen: Das Vertrauen in die Aussage des Anbieters (und damit den Anbieter selbst), dass man sich auf die Systeme verlassen kann, wirft die Frage auf, auf was man sich bei den Systemen verlassen können soll. Hierbei geht es im Rahmen von informationstechnischen Systemen natürlich erst einmal darum, dass sie so funktionieren, wie sie sollen. Betrachtet man es aber aus der Perspektive der Informationssicherheit, geht es vor allem darum, ob die Systeme sicher sind. Ein Credo in der Informationssicherheit ist, dass es keine absolut sicheren informationstechnischen Systeme gibt, daher wird also die höchstmögliche (relative) Sicherheit angepeilt.

Es gibt zwar verschiedene Meinungen darüber, was „vertrauenswürdige Systeme" (lies: verlässliche Systeme vertrauenswürdiger Hersteller) ausmacht, aber kaum Uneinigkeit darüber, was solche informationstechnischen Systeme als sicher qualifiziert. Systeme sollen nachgewiesen sicher sein (u. a. durch qualifizierte Penetrationstests) und nach Möglichkeit nicht durch Bedienfehler – Mangel an Usability – unsicher werden können. Ob diese Systeme dabei aber aus einem bestimmten Land kommen müssen oder der Source-Code für jedermann – und nicht nur für die Prüfenden (den Auditor) – einsehbar sein muss, spielt dabei eine untergeordnete Rolle. Dies wird oft anders dargestellt.

Es kann also ein Nachweis in Eigenregie stattfinden (dann vertraut man sich selbst) oder man vertraut dem Urteil eines Prüfers. Betrachtet man nun den Nachweis von sicheren informationstechnischen Systemen, erkennt man, dass das Vertrauen in den Anbieter keine allzu große Rolle spielt, denn sichere informationstechnische Systeme können nur dadurch entstehen, dass sie ausführlich geprüft werden.

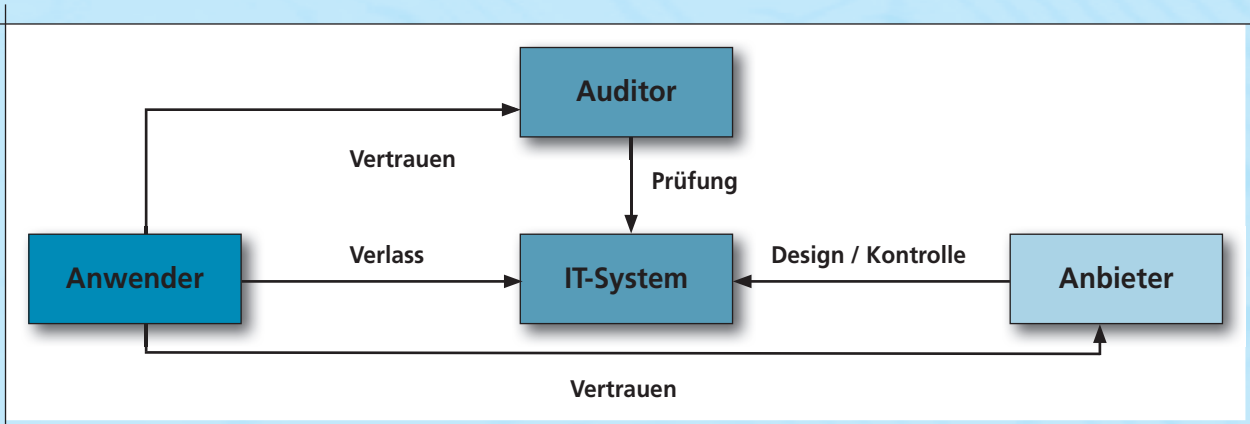

Abbildung 1: Vertrauensverhältnis zwischen Anwender, Anbieter und Auditor

Auch in Gesprächen mit CIOs überwog diese Ansicht, die den bereits genannten, zweiteiligen Prozess wie folgt erweitert:

_____ Prüfung (Kann ich dem Anbieter vertrauen?)

_____ Evaluierung (Prüfung des Systems auf Sicherheit)

und

_____ Risikoabwägung (Kann und will ich das Ergebnis der Evaluierung tragen oder muss ich gegebenenfalls andere Maßnahmen ergreifen?)

Es wird also versucht, so viele Informationen wie möglich über den Anbieter und die Systeme herauszufinden, damit Vertrauen nicht mehr notwendig ist. Anthony Giddens schreibt, die „Hauptbedingung der Vertrauenserfordernisse" sei das „Fehlen vollständiger Informationen" [2]. Sind also (nahezu) vollständige Informationen vorhanden, fällt diese Hauptbedingung der Vertrauenserfordernisse weg.

Es gibt also – nur mittelbar – vertrauenswürdige informationstechnische Systeme, nämlich verlässliche Systeme, die von Anbietern – durch vertrauenswürdige Auditoren nachgewiesen – sicher hergestellt und kontrolliert werden.

Vertrauen in Institutionen der Informationssicherheit

Aus der oben genannten Prämisse lässt sich ableiten, dass nach positiv erbrachtem Nachweis eines vertrauenswürdigen Auditors dem Anbieter vom Anwender Vertrauen entgegengebracht werden kann – obwohl es dann kein Vertrauen mehr benötigt. Auch kann nicht zwingend von dem positiven Ergebnis einer Prüfung auf alle zukünftigen „Produkte" des Anbieters geschlossen werden, weshalb eine stete Prüfung unabdingbar ist – und damit eine Vertrauensbeziehung vom Anwender zum Anbieter weniger beziehungsweise gar nicht zum Tragen kommt. Die Vertrauensbeziehung zwischen Anwender und Auditor ist daher umso wichtiger. Wie kann nun aber dieser Auditor eine gewisse Vertrauenswürdigkeit erlangen?

Zur Evaluierung von Vertrauen in Akteure und Institutionen lohnt sich wieder ein Blick auf den sozialwissenschaftlichen Diskurs solcher Strukturen: Martin Endreß, Professor für Soziologe, diskutiert das Thema aus verschiedenen Perspektiven und charakterisiert an einer Stelle unter Bezug auf Lepsius das Vertrauen in Institutionen wie folgt: „Danach kann sich das Vertrauen zu Institutionen entweder primär auf deren Leitidee, […] auf das Leistungsprofil, also die Performanz bzw. den materiellen Output […] oder auf die konkrete Institutionalisierung […] richten" [3].

In zahlreichen Gesprächen mit CIOs, Hackern und Wissenschaftlern wurde immer wieder das übergeordnete Ziel der transparenten, nachgewiesenen Informationssicherheit als Äquivalent zu dieser Leitidee genannt, welches sich durch die Leistungsprofile „nach außen getragene Kompetenz" (z. B. Veröffentlichung technischer Richtlinien und anderer Informationen, deren Anwendung nachweislich zu mehr IT-Sicherheit führt) und „gute (Krisen-) Kommunikation" auszeichnet sowie von einer Institution verfolgt wird, welche frei von externen Zwängen ist. Wird all dies zusammengeführt, kann man diesem Akteur vertrauen, dass er informationstechnische Systeme sicher prüft.

Ziege und Löwe

Aus sprachlicher Sicht wäre es also nicht korrekt von „vertrauenswürdiger IT" zu sprechen, inhaltlich ist es jedoch unproblematisch, sofern man die Mittelbarkeit beachtet. Unter vertrauenswürdiger IT werden demnach informationstechnische Systeme verstanden, auf deren Sicherheit sich verlassen werden können muss. Diese Verlässlichkeit entsteht durch den Nachweis von Auditoren. Das führt jedoch streng genommen sowohl das mittelbare „Vertrauen" in die Systeme, als auch in deren Anbieter ad absurdum.

Trau, schau, wem? Genau wie in der Äsop-Fabel die Ziege die Situation genau prüft, bevor sie dem Löwen (blind) vertraut, müssen auch informationstechnische Systeme (auf ihre Sicherheit) geprüft werden, bevor sie zum Einsatz kommen. ■

Literatur

[1] Channel Four Television Corporation, Edward Snowden delivers Channel 4's Alternative Christmas Message, News Release, 24. Dezember 2013, www.channel4.com/info/press/news/edward-snowden-delivers-channel-4s-alternative-christmas-message

[2] Anthony Giddens, Konsequenzen der Moderne, Suhrkamp, 1995, ISBN 978-3-518-58197-1

[3] Martin Endreß, Vertrauen (Einsichten. Themen der Soziologie), Transcript Verlag, Bielefeld, 2002, ISBN 978-3-933127-78-5

15. Deutscher IT-Sicherheitskongress

Call for Papers

Der 15. Deutsche IT-Sicherheitskongress des BSI findet vom 16. bis 18. Mai 2017 in der Stadthalle Bonn – Bad Godesberg statt. Der jetzt gestartete „Call for Papers" läuft bis Ende August 2016.

Die Digitalisierung und Vernetzung vieler Lebens- und Arbeitsbereiche geht rasant voran. Gleichzeitig machen technische Innovationen und Entwicklungen in Bereichen wie Industrie 4.0, intelligenten Verkehrssystemen oder im Rahmen der Energiewende deutlich, dass der Sättigungsbereich des möglichen Einsatzes von Informationstechnologie noch lange nicht erreicht ist. Erfolgreich in der Umsetzung können die genannten Entwicklungen aber nur sein, wenn dabei von Anfang an neben funktionalen und ökonomischen Faktoren auch Aspekte der IT-Sicherheit angemessen berücksichtigt werden – Digitalisierung ohne IT-Sicherheit wird am Ende nicht funktionieren.

Beleg dafür, wie angreifbar unsere digitalisierte Gesellschaft ist, sind die zahlreichen Cyber-Angriffe und IT-Sicherheitsvorfälle der letzten Monate. Beispielhaft genannt seien hier die Angriffswellen mit Verschlüsselungs-Trojanern, welche die Daten von tausenden Privatanwendern unbrauchbar gemacht und die geregelten Abläufe in Krankenhäusern, Stadtverwaltungen und Unternehmen teils erheblich beeinträchtigt haben.

Sicherheit ist zwar ein gesellschaftliches Grundbedürfnis, im Falle von IT-Produkten jedoch werden Aspekte der IT-Sicherheit angesichts der rasanten Innovationsgeschwindigkeit und des daraus folgenden ökonomischen Erfolgsdrucks häufig weder von Nutzern noch von Anbietern gleichrangig mitbetrachtet. Die besondere Herausforderung dabei ist, die Sicherheitsziele mit den Nutzeransprüchen in Einklang zu bringen und Produkte zu entwickeln, die den Bedürfnissen der Anwender entsprechen.

Ein Lösungsansatz besteht darin, bei aktuellen Entwicklungen in Bereichen wie Automotive, Industrie 4.0 oder mobilen Anwendungen bereits jetzt Standards zu formulieren, die etablierte Vorgehensweisen und Erkenntnisse in die Produktentwicklung mit einfließen lassen. Nicht zuletzt muss der Verbraucherschutz, also der Schutz der Bürgerinnen und Bürger bei der Nutzung von digitaler Kommunikation und digitalen Diensten, eine besondere Rolle einnehmen. Es gilt für Wirtschaft, Staat und Gesellschaft, einen Mittelweg zwischen zu viel Sicherheit und zu hoher Risikobereitschaft zu finden.

Daher lautet das Motto des 15. Deutschen IT-Sicherheitskongresses:
Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis

Mit über 600 Fachbesuchern (im Jahre 2015) ist der Deutsche IT-Sicherheitskongress, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) alle zwei Jahre ausrichtet, eine feste Größe im Veranstaltungskalender der IT-Sicherheitsbranche. Drei Tage lang diskutieren die Teilnehmer über den Stand der nationalen und internationalen Entwicklung zur IT-Sicherheit. Ziel des Kongresses ist es, das Thema IT-Sicherheit aus unterschiedlichen Blickwinkeln zu beleuchten, Lösungsansätze vorzustellen und weiterzuentwickeln. Eine begleitende Ausstellung ergänzt das Vortragsprogramm.

Für den Kongress 2017 sucht das BSI kreative, praxisnahe und verständliche Beiträge, die sich mit Themen wie Automotive, Industrie 4.0, mobile Anwendungen oder einem der folgenden Themenbereiche auseinandersetzen:

Cyber-Sicherheit

- Cyber-Angriffe: Trends, Prävention, Detektion und Reaktion
- Advanced Persistent Threats: Vorgehensweisen und Schutzmöglichkeiten
- Sichere Internet-Infrastruktur

Termine

Vortragsanmeldung mit Abgabe von Gliederung und Kurzfassung bis zum	31. August 2016
Review der eingereichten Beiträge durch den Programmbeirat bis zum	11. November 2016
Benachrichtigung der Autorinnen und Autoren ab dem	5. Dezember 2016
Einsendeschluss für die druckreife Langfassung bis zum	31. Januar 2017

_____ Resistenz von Internet-Browsern gegen moderne Angriffstechniken und Abwehr
_____ Incident-Management/-Handling, Forensik, Revision, Penetrationstests
_____ Schutz kritischer Infrastrukturen – Architektur, Organisation, Technik

Zertifizierung und Standards

_____ Zertifizierung von Produkten, Dienstleistungen und Personen im Zeitalter der Digitalisierung
_____ Zertifizierung im internationalen Kontext, Prävention statt Reaktion – Sicherheit durch Zertifizierung
_____ Branchenspezifische Sicherheitsstandards
_____ Prüfstandards in Gesetzesvorhaben – rechtliche und technische Implikationen und Best Practices

Sichere Identitäten

_____ Digitale Identitäten für eine vernetzte Welt
_____ Biometrie: Technik und Eigenschaften
_____ Identitäten in E-Government und hoheitlichen Infrastrukturen
_____ Skalierbare eID-Architekturen in unterschiedlichen Anwendungsfeldern

Sicherheit von Plattformen, Firmware und Betriebssystemen

_____ Firmware: Angriffe, Vertrauenswürdigkeit und Integrität
_____ Administration und Kontrolle von Schnittstellen
_____ Protokollierung von Ereignissen, protokollierbare Charakteristika von Angriffen
_____ Sichere Enklaven: Isolation von Betriebssystemen, Komponenten und Anwendungen
_____ Hardware-Sicherheitsanker und sicheres Booten

Management von Informationssicherheit

_____ Risiko-Management: Herausforderungen und Lösungen
_____ Business-Continuity-Management
_____ Sicherheitsteams: Aufgaben, Kompetenzen, Organisation
_____ Benchmarking und Messbarkeit von Informationssicherheit
_____ Status quo der Informationssicherheit: Self-Assessment, externe Revision, Audits

Industrielle Sicherheit / Internet der Dinge (IoT)

_____ Sicherheit von Industrie 4.0
_____ Embedded Systems, Cyber-Physical-Systems und Sicherheit
_____ SCADA-Netze, Anbindung an Unternehmensnetze
_____ Embedded Defense
_____ Automotive Security – Sicherheit autonomer Mobilität

Sichere mobile Kommunikation

_____ App-Sicherheit
_____ Mobile Payment
_____ Kommunikationsstandards: WLAN, Near-Field-Communication, Bluetooth, DECT et cetera
_____ Trusted Execution-Environment, Secure Elements
_____ Sicherheit von Commercial-off-the-Shelf-(COTS)-Produkten

Benutzbare sichere IT-Systeme

_____ Aktuelle Trends in „Usable Security“
_____ Anwendertaugliche Ende-zu-Ende-Verschlüsselung
_____ TLS – Umgang mit Warnungen, Anforderungen und Migration
_____ Plattformübergreifende Anwendungs-, Patch- und Updateverwaltung
_____ Sichere Netzanbindung beim Anwender (WLAN, Router etc.)

Sicherheitsmonitoring in kryptografisch geschützten Systemen

_____ Auswertung von sicherheitskritischen Systemereignissen und Kommunikationsflüssen
_____ Big Data und Machine-Learning im Kontext Intrusion-Detection
_____ Security-Information- und -Event-Management (SIEM) auf verteilten Plattformen

IT-Sicherheit in der Gesellschaft

_____ Neue Konzepte und Erfolgsstrategien zur Sensibilisierung, internationale Ansätze
_____ Datensicherheit im digitalisierten Leben – von Smart Devices bis Wearables
_____ Datenschutz und Informationssicherheit – Zusammenspiel und Spannungsverhältnis
_____ Resilienz 2.0: Gesellschaft und Informationssicherheit
_____ Bedeutung von Vertrauen in der Informationssicherheit

IT-Sicherheit und Recht

_____ Rechtliche Anreize als Instrumente zur Förderung der IT-Sicherheit

- Nationale IT-Souveränität und Grenzen nationaler Regulierung im Cyber-Raum
- Wie kann Recht die Bildung von Vertrauen in IT unterstützen?
- Verantwortungsteilung zwischen Herstellern, Nutzern und Dienstleistern

Sicheres Cloud Computing

- Auditierung von Cloud-Anbietern: Best Practices und neue Ansätze
- Sichere Authentifizierung von Cloud-Nutzern: Single Sign-on, Federation-Service
- Zwei-Faktor-Authentifizierung, Mobile Devices
- Behandlung von Sicherheitsvorfällen in der Cloud: Herausforderungen für CERTs
- Software-Defined-Network und Software-Defined-Data-Center: Chancen und Risiken
- Cloud Forensik: Möglichkeiten und Grenzen

Die Liste der Themen ist nicht abschließend; gerne können Sie Beiträge auch zu anderen Themen der IT-Sicherheit einreichen. Die Beiträge sollen praxisnah,

Programmbeirat

Zu den vom BSI berufenen Mitgliedern des Programmbeirates gehören

Dr. Rainer Baumgart
secunet Security Networks AG

Prof. Dr. Christoph Busch
Competence Center for Applied Security Technology CAST e. V.

Dr. Walter Fumy
Bundesdruckerei GmbH

Winfried Holz
BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Prof. Dr. Klaus-Peter Kossakowski
HAW Hamburg/DFN-CERT Services GmbH

Dieter Schweer
Bundesverband der Deutschen Industrie e. V.

Prof. Dr. Peter Martini
Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)

Prof. Dr. Alexander May
Lehrstuhl für Kryptologie und IT-Sicherheit Ruhr-Universität Bochum

Dr. Gisela Meister
Giesecke & Devrient GmbH

Dr. Klaus Mittelbach
ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Dr. Holger Mühlbauer
TeleTrusT – Bundesverband IT-Sicherheit e. V.

Prof. Dr. Reinhard Posch
Technische Universität Graz
Chief Information Officer (CIO) der österreichischen Bundesregierung

Prof. Michael Rotert
eco – Verband der deutschen Internetwirtschaft e. V.

Jürgen Schmidt
heise Security

François Thill
Direction du commerce électronique et de la sécurité informatique

Andrea Voßhoff
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Dr. Gerhard Weck
INFODAS – Gesellschaft für Systementwicklung und Informationsverarbeitung mbH

Winfried Wirth
Rohde & Schwarz SIT GmbH

Klaus-Dieter Wolfenstetter
Deutsche Telekom AG

Steffen Zimmermann
Verband Deutscher Maschinen- und Anlagenbau e. V.

Für Fragen und Anregungen können Sie gerne Kontakt mit dem BSI aufnehmen unter Telefon +49 22899 9582-5365 oder kongress2017@bsi.bund.de.

aktuell und möglichst auch für Personen aus dem weiteren IT-Sicherheitsumfeld verständlich sein.

Einreichung von Beiträgen

Wenn Sie einen Beitrag einreichen möchten, so beachten Sie bitte folgende Rahmenbedingungen:

_____ Bitte senden Sie uns eine Gliederung und Kurzfassung des Beitrages unter Nennung des Themengebietes im Umfang von drei bis vier DIN-A4-Seiten in elektronischer Form an papers2017@bsi.bund.de.

_____ Die Einreichungen werden durch den Programmbeirat anonym begutachtet und bewertet. Folgende Daten müssen daher gesondert aufgeführt werden und dürfen nicht im Beitrag enthalten sein: Name, Unternehmen/Institution, vollständige Adresse, Telefonnummer, E-Mail-Adresse

Bewertungskriterien

_____ Beitrag entspricht den formalen Aspekten
_____ Ist das Thema aktuell und kein PR-Beitrag?
_____ Wie wird der wissenschaftliche Wert des Beitrags beurteilt?
_____ Wie wird der praktische Wert des Beitrags beurteilt?
_____ Löst der Text die im Titel gestellte Aufgabe?
_____ Ist der Beitrag übersichtlich und gut gegliedert?
_____ Ist das Abstract verständlich? (prägnant formuliert, mit angemessenem Aufwand lesbar – wird auf Beispiele hingewiesen, die in der Langfassung ausgeführt werden?)

Bei Annahme eines eingereichten Beitrages durch den Programmbeirat werden Sie darüber informiert und gebeten, eine Langfassung (8–15 Seiten) zu erstellen und zu übersenden. Die Langfassung wird im Tagungsband veröffentlicht. Im Rahmen der Veranstaltung erhalten die Autorinnen und Autoren Gelegenheit, ihren Beitrag in einem circa 20-minütigen Vortrag mit anschließender Diskussion vorzustellen.

Best-Student-Award

Auch Studierende sind dazu aufgerufen, Beiträge einzureichen. Als Preis für den Best-Student-Award wird ein dreimonatiger Forschungsaufenthalt gestiftet, der zudem mit einem Preisgeld unterstützt wird. Entsprechende Beiträge müssen deshalb als solche gekennzeichnet sein.

Format

Bitte achten Sie darauf, dass die Beiträge/Dateien in einem für OpenOffice oder Word kompatiblen Format übermittelt werden. Beiträge, die den oben genannten Vorgaben nicht entsprechen, können nicht berücksichtigt werden. ■

kurz notiert

Themenpapier zu Ransomware

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Themenpapier zu Ransomware veröffentlicht. Vor dem Hintergrund der aktuellen IT-Sicherheitsvorfälle durch Verschlüsselungs-Trojaner beschreibt das Themenpapier die verschärfte Bedrohungslage durch Ransomware und stellt Angriffsvektoren und mögliche Schäden dar. Weiterer Schwerpunkt des Papiers sind konkrete Empfehlungen und Hilfestellungen für die Prävention und die Reaktion im Schadensfall. Das Themenpapier richtet sich an professionelle Anwender und IT-Verantwortliche in Unternehmen, Behörden und anderen Institutionen.

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. „ransom“) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

„Die durch Ransomware verursachten IT-Sicherheitsvorfälle der letzten Wochen zeigen, wie abhängig Unternehmen und andere Institutionen von Informationstechnologie sind und welche Auswirkungen ein Cyber-Angriff haben kann. Das BSI ruft IT-Anwender auf, sich mit der aktuellen Bedrohungslage durch Ransomware auseinander zu setzen und entsprechende Schutzmaßnahmen zu ergreifen. Das Themenpapier Ransomware leistet dazu eine pragmatische und wertvolle Hilfestellung“, erklärt Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Das Themenpapier steht über www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf;?__blob=publicationFile&v=2 zum kostenlosen Download zur Verfügung. ■

Amtliche Mitteilungen

1. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen sind inzwischen folgende Zertifizierungen des BSI gemäß Common Criteria und ITSEC abgeschlossen worden:

Hersteller/Vertreiber	Produkt	Produkt-Typ	Ergebnis ID Zertifizierungsdatum
Infineon Technologies AG	Infineon Technologies AG Smartcard IC (Security Controller) M5072 G11 including optional Software Libraries RSA-EC-Toolbox	Smartcard Controller	BSI-DSZ-CC-0946-V2-2015-MA-01 2016-03-15
genua GmbH	genuscreen 5.0	Firewall	BSI-DSZ-CC-0966-2015-MA-01 2016-03-11
secunet Security Networks AG	secunet wall packet filter, Version 5.1.0	Packet Filter	EAL4+ BSI-DSZ-CC-0991-2016 2016-03-10
Broadcom Corporation	BCM_SPS02 Secure Processing System with IC Dedicated Software, Version 1.0	Secure Processing System	EAL5+ BSI-DSZ-CC-0915-2016 2016-02-25
SUSE LLC	SUSE Linux Enterprise Server, Version 12	Betriebssystem	EAL4+ BSI-DSZ-CC-0962-2016 2016-02-24
NXP Semiconductors Germany GmbH	NXP Secure Smart Card Controller P60D024/016/012yVB(Y/Z/A)/yVF with IC Dedicated Software	Smartcard Controller	EAL6+ BSI-DSZ-CC-0939-V2-2016 2016-02-18
NXP Semiconductors Germany GmbH	NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software	Smartcard Controller	EAL6+ BSI-DSZ-CC-0978-2016 2016-02-05
Giesecke & Devrient GmbH	STARCOS 3.6 COS C1	Smartcard mit Anwendung (eHealth)	BSI-DSZ-CC-0916-2015-MA-01 2016-01-28
Infineon Technologies AG	Infineon Technologies AG Trusted Platform Module SLB9670_2.0, v7.40.2098.00	Trusted Platform Module	EAL4+ BSI-DSZ-CC-0998-2016 2016-01-28
Microsoft Corporation	Microsoft SQL Server 2014 Database Engine Enterprise Edition x64 (English) 12.0.4100.1	Datenbankserver	EAL 4+ BSI-DSZ-CC-0929-2015 2015-12-15
IBM Corporation	IBM WebSphere DataPower Firmware,Version 6.0.2.0	Netzwerkanwendung	EAL 4+ BSI-DSZ-CC-0901-2015 2015-12-09

Anmerkung:

– Die zugehörigen Zertifizierungsreporte mit Zertifikaten sind auf der Web-Seite www.bsi.bund.de/zertifizierungsreporte einzusehen.

2. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen ist inzwischen für folgende Produkte eine Zertifizierung beantragt worden:

Antragsteller	Produktname	Produkttyp	Zertifizierungs-ID
OpenLimit SignCubes AG	Open Limit Anwendungs-konnektor Version 1.0	Anwendungskonnektor	BSI-DSZ-CC-1009
Dell Inc.	Dell EqualLogic TS 4000 Series Storage Firmware v7.1.1	Other devices and Systems	BSI-DSZ-CC-1008
Microsoft Corporation	SQL Server 2016 Database Engine Enterprise Edition x64 (English)	Database Management System (DBMS)	BSI-DSZ-CC-1004
Gemalto SA	Smart Meter Gateway SM applet on platform named MultiApp V4	Smart Meter Security Module	BSI-DSZ-CC-1003
IBM Corporation	IBM Enterprise PKCS#11IBM Enterprise PKCS#11	Cryptographic Module	BSI-DSZ-CC-1002

Anmerkungen:

- Eine Veröffentlichung dieser Angaben erfolgt hier nur, sofern der Antragsteller damit einverstanden ist *und* die Evaluierung begonnen wurde. In der Liste vorhandene Nummerierungslücken betreffen beantragte Zertifizierungen, für die die genannten Voraussetzungen fehlen.
- Bei einigen Produkten handelt es sich um eine Re-Zertifizierung eines bereits zertifizierten Produktes wegen Änderungen am Produkt oder Wechsel der Prüfkriterien.

3. Vom BSI erteilte Standortzertifikate

Antragsteller	Entwicklungs-/ Produktionsstandorte	ID Ausstellungsdatum	gültig bis
Giesecke & Devrient GmbH	Giesecke & Devrient Secure Data Management GmbH, Austraße 101b, 96465 Neustadt bei Coburg	BSI-DSZ-CC-S-0058-2016 2016-03-03	2018-03-02
Ardentec Corporation	Ardentec Corporation, Ting-Sing site (T Site) and Kaiyuan site (K Site)	BSI-DSZ-CC-S-0054-2016 2016-01-07	2018-01-06
SMARTRAC TECHNOLOGY Ltd.	SMT1, SMARTRAC TECHNOLOGY Ltd. (Thailand), 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang-pa-In, 13160 Ayutthaya, Thailand	BSI-DSZ-CC-S-0057-2015 2015-12-28	2017-12-27

4. Vom BSI erteilte ISO-27001-Zertifikate auf der Basis von IT-Grundschutz

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0216-2016	DTS IT AG	Der Informationsverbund der DTS IT AG umfasst den Betrieb und das Management des Rechenzentrums am Standort Herford. Der Untersuchungsgegenstand ist die DTS Systeme GmbH mit den Kernaufgaben im Betrieb und Management des Rechenzentrums und der verbundenen Dienstleistungen. In der Definition des IT-Verbundes werden sämtliche Server, Netzwerkkomponenten, Client-systeme, Anwendungen, Netze, Gebäude und Räume integriert.	2019-03-06

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0225-2016	1&1 De-Mail GmbH	Die 1&1 De-Mail GmbH bietet für die Marken WEB.DE, GMX und 1&1 einen De-Mail-Dienst nach den Technischen Richtlinien De-Mail und dem De-Mail-Gesetz an. Der De-Mail-Dienst besteht aus einem Postfach- und Versanddienst (PVD) für den Empfang und den Versand standardisierter rechtssicherer elektronischer Nachrichten, einem Accountmanagement (ACM) zur Verwaltung von Kundendaten sowie einer sicheren IT-Basisinfrastruktur (IT-BInfra). Der De-Mail-Dienst erfüllt die Anforderungen an Funktionalität und Interoperabilität für einen De-Mail-Dienstanbieter. Die Administration des De-Mail-Dienstes erfolgt am Standort Karlsruhe, wobei sich die Rechenzentren für den hochverfügbaren Dienst in Frankfurt am Main befinden. Das De-Mail-Angebot der 1&1 De-Mail GmbH richtet sich an private Kunden der 1&1 Mail&Media GmbH mit ihren Marken WEB.DE und GMX sowie an Geschäftskunden der 1&1 Internet SE mit der Marke 1&1.	2019-03-03
BSI-IGZ-0221-2016	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH	Der Untersuchungsgegenstand umfasst den Betrieb der Basis-Systeme für die Fachanwendungen der Landesverwaltung M-V und des DVZ selbst sowie weiterer Kunden am Standort Schwerin. Neben diesen Basis-Systemen, welche aus physikalischen und virtuellen Servern bis zur Betriebssystemebene sowie Datenbanken und Webservern bestehen, gehören auch alle für den Betrieb erforderlichen Infrastrukturen- und Sicherheits-Services zum Untersuchungsgegenstand. Diese sind unter anderem die Netzwerkinfrastruktur (inkl. dem landesweiten MPLS-Netz „CN-LAVINE“), SAN, Netzwerk- und Systemverwaltung, zentraler Internetzugang, Groupwaredienste sowie die gesamte Bürokommunikation des DVZ.	2019-02-11
BSI-IGZ-0218-2016	neu-itec GmbH	Der Untersuchungsgegenstand umfasst Infrastruktur, Anlagen und Leistungen der neu-itec GmbH Neubrandenburg, die für die Erbringung von IT-Dienstleistungen entsprechend des Produktportfolios wesentlich sind. Dazu gehören Server, Netze, Netzkomponenten und Arbeitsplatzsysteme in den Räumen der neu-itec GmbH Neubrandenburg und alle unterstützenden Prozesse wie zum Beispiel Datensicherung, Netzmanagement und Systembetreuung.	2019-01-28
BSI-IGZ-0226-2016	KomIT URS	Alleiniges Geschäftsziel der KomIT URS ist der Betrieb von IT-Systemen und Anwendungen im Auftrag der Zweckverbände Kommunale Datenverarbeitung Region Stuttgart (KDRS) und Kommunale Informationsverarbeitung Reutlingen-Ulm (KIRU) und ihrer Betriebsgesellschaften Rechenzentrum Region Stuttgart GmbH (RZRS) und Interkommunale Informationsverarbeitung Reutlingen-Ulm GmbH (IIRU), die wiederum im Auftrag der Landkreise, Städte, Gemeinden, deren Unternehmen und Verbänden in Baden-Württemberg handeln. Komponenten sind Server, darauf installierte Anwendungen, Netzwerk und Security-Gateways an dessen Grenzen. Als zusätzliche Komponente kommt das gemeinsame Hausnetz der jeweiligen Betriebs-GmbH dazu, da daraus Administrationstätigkeiten der KomIT URS erfolgen. Auswahl der Verfahren und der eingesetzten Software sowie Service Design (nach ITIL) ist nicht Gegenstand des IT-Verbundes. Insofern ist lediglich die Infrastruktur, nicht das jeweilige Verfahren beziehungsweise die dazugehörige Anwendungssoftware Teil des IT-Verbundes. Nur wenn Software unter der vollständigen Kontrolle des Informationssicherheitsmanagementsystemes des IT-Verbundes KomIT URS steht und somit durch den Auftraggeber die Verantwortlichkeit für Security vollständig an KomIT URS übertragen ist, werden Applikationen in den IT-Verbund übernommen.	2019-01-21