BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Messepräsenz

Das BSI auf der it-sa 2017

Vom 10. bis 12. Oktober 2017 ist das BSI mit einem Stand und Vortragsaktivitäten auf der it-sa in Nürnberg vertreten. Das BSI fungiert gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM e. V.) als ideeller Träger.

Am BSI-Stand in Halle 10, Stand 101 können Sie sich zu folgenden Themen informieren:

5 Jahre Allianz für Cyber-Sicherheit

Im Jahr 2012 beschlossen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Digitalverband BITKOM die Grundsteinlegung für die Allianz für Cyber-Sicherheit. Seitdem haben sich der Initiative über 2400 Organisationen angeschlossen. Sie profitieren vom Austausch mit IT-Sicherheitsexperten und nutzen Informationen über aktuelle Cyber-Bedrohungen.

Am 10. Oktober feiert die Allianz für Cyber-Sicherheit darüber hinaus ihr fünfjähriges Bestehen. Die BSI-Mitarbeiter nehmen dies zum Anlass, um Einblicke in die tägliche Arbeit der Initiative und kommende Vorhaben zu geben.

Cloud-Computing

„Cloud Computing Compliance Controls Catalogue" – kurz C5 – heißt der Anforderungskatalog für sicheres Cloud-Computing des BSI. Seine Sicherheitsanforderungen für professionelle Cloud-Dienste basieren auf internationalen Standards, ergänzt um Anforderungen des BSI. Fachlich qualifizierte Wirtschaftsprüfer testieren auf Grundlage der Norm ISAE 3000 die Einhaltung des C5, was sich nachweislich gut mit anderen Prüfungen kombinieren lässt. Einige Cloud-Anbieter sind bereits testiert, C5 ist zudem eine Säule für das europäische Cloud-Label ESCloud, das zusammen mit der französischen Partnerbehörde ANSSI etabliert wird.

IT-Grundschutz

Zum Abschluss der Modernisierung des IT-Grundschutzes stellt das BSI im Rahmen der Security-Messe it-sa die Schwerpunkte und neuen Entwicklungen der bewährten BSI-Methode vor:

Die drei modernisierten BSI-Standards 200-1, 200-2 und 200-3 werden zur it-sa in einer neuen Print-Auflage erscheinen. Das IT-Grundschutz-Kompen-

Inhalt

Impressum

Redaktion:
Nora Basting (verantwortlich)
E-Mail: nora.basting@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Referat Cyber-Sicherheit für den Bürger
und Öffentlichkeitsarbeit
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
25. Jahrgang 2017

dium mit rund 80 Bausteinen wird vorgestellt. Die Bausteine enthalten nun Basis- und Standard-Anforderung sowie Anforderungen für den erhöhten Schutzbedarf.

Einen Einstieg in den IT-Grundschutz und die Basis-Absicherung ermöglicht der „Leitfaden zur Basis-Absicherung“: Mit der neuen Publikation können besonders Anfänger und Einsteiger mit dem Aufbau eines Managementsystems zur Informationssicherheit (ISMS) beginnen.

Am 11. Oktober 2017 findet zudem der vierte IT-Grundschutz-Tag des Jahres statt. Die in Kooperation mit dem Bundesanzeiger Verlag geplante Veranstaltung wird ebenfalls Ergebnisse der IT-Grundschutz-Modernisierung vorstellen. Neben der Veranstaltung werden am BSI-Messestand die IT-Grundschutz-Experten des BSI für Fragen zur Verfügung stehen.

Weitere Fachpräsentationen am BSI-Messestand:

_____ Schutz kritischer Infrastrukturen
_____ IT-Sicherheitszertifizierung
_____ Sicheres mobiles Arbeiten
_____ Sicherheitsberatung

BSI-Vorträge zu aktuellen Themen der IT-Sicherheit:

Mittwoch, 11. Oktober 2017,
Halle 10, Forum Rot, 09:30–09:45 Uhr
Cloud-Sicherheit
Dr. Clemens Doubrava, BSI

Donnerstag, 12. Oktober 2017,
Halle 10, Forum Rot, 09:15–09:30 Uhr
Allianz für Cyber-Sicherheit
Stephan Becker, BSI

Taxonomie

BSI empfiehlt eine neue, zeitgemäße Rechenzentrums-Definition

In den letzten Jahrzehnten haben sich Aufbau, Struktur und technische Ausstattung von Rechenzentren umfassend verändert. Für das BSI war es deswegen an der Zeit, die aus der Mitte der 1990er-Jahre stammenden Definitionen der Begriffe „Rechenzentrum“ und „Serverraum“ neu zu fassen. So können Empfehlungen und Vorgaben – beispielsweise im IT-Grundschutz oder in den Mindeststandards nach § 8 Abs. 1 BSIG – praxisnäher formuliert werden.

Von Frank Weber und Dr. Markus Held, BSI

Eine klare und zeitgemäße Festlegung, welche Infrastrukturbereiche als Rechenzentrum zu gelten haben, ist für Unternehmen und Behörden gleichermaßen von Bedeutung, denn sowohl Management-Entscheidungen (z. B. bei IT-Investitionen) als auch die Interpretation normativer Vorgaben werden oft davon beeinflusst. Hierfür werden praxisorientierte Kriterien benötigt, mit denen sich relevante Infrastrukturbereiche nachvollziehbar und zuverlässig als Rechenzentrum identifizieren und klassifizieren lassen.

Die aus den Anfangsjahren des IT-Grundschutzes stammenden Definitionen zum Rechenzentrum (RZ) und Serverraum (SR) sind angesichts der sich veränderten IT-Landschaft nicht mehr zeitgemäß und verlieren zunehmend ihre praktische Anwendbarkeit. Zudem setzt die seit 2014 schrittweise in Kraft gesetzte DIN EN 50600 als „RZ-Norm“ einen neuen Rahmen, mit dem die alte Definition aus dem IT-Grundschutz nicht mehr in Einklang steht. Eine ganz wesentliche Eigenschaft der neuen RZ-Norm ist es, (in DIN EN 50600-1 unter Nummer 3.1.9) den Begriff des Rechenzentrums sehr weit zu fassen und bewusst an Funktionalität statt an der Ausführungsform oder Größe auszurichten. Damit enthebt sich die Norm der Notwendigkeit, zwischen Rechenzentrum und Serverraum zu unterscheiden.

Eine weitere Motivation, die Definition eines Rechenzentrums zu überarbeiten, ergab sich aus dem Projekt „IT-Konsolidierung Bund“. Darin wurde das BSI vom Haushaltsausschuss des Deutschen Bundestags zum einen mit der Analyse der bestehenden Rechenzentren in

der Bundesverwaltung beauftragt. Zum anderen erging der Auftrag einen „Mindeststandard nach § 8 Abs. 1 BSIG zu erarbeiten, der die Anwendung des ‚HV-Benchmark kompakt 3.0' für die Stellen des Bundes" regelt – der Mindeststandard wurde am 26. Mai 2017 vom BSI veröffentlicht [3].

Beide Aufträge machten es erforderlich, die aus der Mitte der 1990er-Jahre stammenden Definitionen für Rechenzentrum und Serverraum zu überarbeiten und neu zu fassen. Dabei wird der bisherige Ansatz, die Unterscheidung zwischen RZ und SR über getroffene Maßnahmen, Organisationsformen oder Betriebsgrößen zu definieren, fallengelassen. Die neue Definition [1] orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der nutzenden Organisation und steht damit im methodischen Einklang mit der DIN EN 50600.

RZ-Definition

(1) Hat eine IT-nutzende Organisation nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein RZ entsprechend dem Schutzbedarf zu behandeln. Unter „IT-Betriebsbereich" sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das RZ umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik etc.), die dem bestimmungsgemäßen Betrieb und der Sicherheit des IT-Betriebsbereichs dienen.

(2) Wird die IT der Organisation innerhalb eines Gebäudes / einer Liegenschaft verteilt in mehreren Bereichen betrieben und sind diese Bereiche untereinander und zu den IT-Nutzern hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als RZ zu behandeln. Das sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr Nutzer abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden.

(3) Ist die IT-nutzende Organisation an mehreren, räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend (1) separat zu betrachten und zu behandeln.

(4) Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben einer Organisation führen) erforderliche IT angesiedelt ist, ist immer als RZ zu behandeln, unabhängig von Größe oder Anteilsregeln aus Nummer (2).

(5) IT-Betriebsbereiche, aus denen heraus Dienste/Dienstleistungen für Dritte erbracht werden, sind immer als RZ zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht.

(6) Besteht ein begründetes Interesse, einen IT-Betriebsbereich gemeinsam mit seinem Supportbereich abweichend von den vorgenannten Regelungen als Serverraum zu behandeln, ist dies samt der sich daraus ergebenden Reduzierungen von Maßnahmen der IT-Sicherheit anhand einer Risikoanalyse zu begründen.

Der schon angesprochene Mindeststandard nutzt bereits diese neue Definition in einer vereinfachten Form. Somit können Bundesbehörden bei der Umsetzung des Mindeststandards bereits den neuen Ansatz nutzen. ■

Literatur

[1] BSI, Rechenzentrums-Definition, 2017, www.bsi.bund.de/RZ-Definition

[2] BSI, IT-Grundschutz – Community Drafts: Baustein INF (Infrastruktur), www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/GS_Drafts/INF/inf_drafts_node.html

[3] BSI, Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG, www.bsi.bund.de/mindeststandards

Allianz für Cyber-Sicherheit:

Seit fünf Jahren gemeinsam gegen Cyber-Bedrohungen

Mehr Schutz vor Cyber-Angriffen für deutsche Institutionen ist das Hauptanliegen der Allianz für Cyber-Sicherheit. Dieses Jahr feiert die Initiative ihren fünften Geburtstag. Ein Rückblick auf bislang Erreichtes und kommende Aufgaben.

Als das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) im Jahr 2012 die Gründung der Allianz für Cyber-Sicherheit bekanntgaben, führte dies vielerorts lediglich zu einer Randnotiz. Schließlich galt das Hauptanliegen der Initiative – mehr Schutz für deutsche Institutionen vor Cyber-Angriffen – bis dahin eher als thematische Nische: In der Regel hatten vor allem international agierende Großkonzerne oder aber Unternehmen, deren Chefetagen ein Faible für Verschwörungstheorien und „Big Brother is watching you"-Fantasien übrig hatten, die Notwendigkeit von Schutzmaßnahmen gegen Hacker-Angriffe erkannt.

Bei anderen Geschäftsführern – insbesondere aus kleinen und mittelständischen Unternehmen – war dieses Thema allenfalls weit unten auf der Agenda: Die vermeintlich geringe Bekanntheit auf dem internationalen wirtschaftlichen Parkett galt als ausreichender Schutzwall. Betroffen waren schließlich immer nur die dicken Fische.

Einige Monate später brachte Edward Snowden die Praktiken von NSA und anderen Geheimdiensten ans Licht: Wer zuvor noch müde belächelt worden war, weil er E-Mails verschlüsselte und sich in sozialen Netzwerken zurückhielt, konnte sich mit einem „Ich hab es euch ja immer gesagt" brüsten. Wer sich bis dato gutmütig (oder eben blauäugig) in der virtuellen Welt verhalten, Geschäftsgeheimnisse ungeschützt über das WWW verteilt oder aus Bequemlichkeit sogar seine Produktionsanlagen direkt an das Internet gekoppelt hatte, wurde nun eines Besseren belehrt.

Plattform für Information und Austausch

An dieser Stelle setzt die Allianz für Cyber-Sicherheit (ACS) an: Unternehmen und andere Organisationen, die Informationen zum Schutz ihrer IT vor Angriffen aus dem Cyber-Raum suchen, finden unter dem Dach der Initiative zahlreiche kosten- und werbefreie Angebote. Als Informationspool dient insbesondere die Webseite www.allianz-fuer-cybersicherheit.de: Sowohl das BSI als auch verschiedene Partner aus der IT-Branche mit ausgewiesener Expertise bieten dort umfangreiche Hinweise zu aktuellen IT-Sicherheitsthemen an. Mal steht die Prävention im Fokus – zum Beispiel bei der sicheren

Cyber-Sicherheits-Umfrage 2017: Aufruf zur Teilnahme

Aus Angst davor, dass die eigene Reputation Schaden nehmen könnte, werden Cyber-Angriffe in vielen Fällen immer noch verschwiegen. Auch wenn einige Vorfälle doch noch an die Öffentlichkeit gelangen, ist die Dunkelziffer der von Cyber-Kriminellen ins Visier genommenen Unternehmen Schätzungen zufolge weitaus höher, als dies aus der Fachpresse hervorgeht. Um einen genaueren Überblick über die Betroffenheit deutscher Institutionen durch Angriffe aus dem WWW zu erhalten, führt die Allianz für Cyber-Sicherheit jährlich eine Cyber-Sicherheits-Umfrage durch.

Hier soll versucht werden, Informationen zur tatsächlichen Betroffenheit durch Cyber-Angriffe, zur subjektiven Gefährdungslage und zum Umsetzungsstand von Schutzmaßnahmen aus Sicht von Unternehmen, Behörden und anderen Institutionen zu erhalten. Aus den Ergebnissen der Umfrage lassen sich unter anderem praxisbezogene Lösungsansätze und Empfehlungen sowie Beratungsschwerpunkte ableiten. Zudem fließen die Ergebnisse der Umfrage als weiterer Baustein in die Erstellung und kontinuierliche Pflege eines Lagebilds der Cyber-Sicherheit in Deutschland ein. Wir würden uns freuen, wenn Sie sich die Zeit nehmen würden, um den Fragebogen auszufüllen. Alle Angaben sind freiwillig und völlig anonym. *(www.cyber-sicherheits-umfrage.de)*

Konfiguration von IT-Systemen –, mal die Reaktion auf gegenwärtige Bedrohungen, was nicht zuletzt auch in der Verteilung von BSI-Warnmeldungen an die Mitglieder der Allianz für Cyber-Sicherheit mündet. Viele Hinweise werden zum Nachlesen, einige auch als Seminare oder Video angeboten.

Neben der Information von Institutionen ist der Austausch untereinander ein wichtiges Standbein der Initiative. Mitglieder können sich in kleinen Gruppen zusammenschließen und branchen- oder themenspezifische Arbeitskreise – im Allianz-Terminus „Erfahrungsaustausch-" beziehungsweise „Expertenkreise" genannt – gründen. Diese tagen in regelmäßigen Abständen, helfen den Beteiligten, voneinander zu lernen, und erzeugen mitunter Resultate, die wiederum auf der Webseite zur Verfügung gestellt werden können.

Zu aktuellen Themenschwerpunkten, die für alle Mitglieder von Interesse sind, bietet die Allianz außerdem regelmäßige Cyber-Sicherheits-Tage an, die an wechselnden Standorten in ganz Deutschland stattfinden. So trifft man sich beispielsweise am 7. November 2017 in Stuttgart, um mit Fachvorträgen und Workshops über das Thema „Cloud" zu informieren. Aber auch andere Orte in Deutschland, wie Dortmund, Berlin, Hamburg oder Leipzig, dienten schon als Treffpunkt für Cyber-Sicherheits-Tage.

Ungebrochener Zulauf

Seit der Gründung der Allianz für Cyber-Sicherheit haben sich der Initiative inzwischen über 2400 Unternehmen und Institutionen aus Deutschland angeschlossen. Der Großteil davon als Nutzer der Angebote (Teilnehmer), circa 100 Unternehmen steuern selbst Inhalte bei (Partner) und mehr als 40 engagieren sich als so genannte Multiplikatoren, die Informationen zur Allianz für Cyber-Sicherheit und deren Angebote an andere Institutionen weiterverteilen. Hierbei handelt es sich häufig um Verbände, Presseorgane oder Ähnliches.

Das Engagement der Beteiligten ist beachtlich: Über 300 Dokumente wurden in den vergangenen fünf Jahren von den Partnern der Allianz für Cyber-Sicherheit und dem BSI erstellt und über den Informationspool zur Verfügung gestellt. In den vergangenen drei Jahren fand durchschnittlich an jedem fünften Tag ein Event zum Thema „Cyber-Sicherheit" statt, das von der Allianz selbst oder einem Partner organisiert wurde. Die offiziellen Cyber-Sicherheits-Tage sind in der Regel innerhalb von wenigen Tagen, ausgewählte Fortbildungen, wie das Übungszentrum Netzverteidigung, sogar innerhalb weniger Stunden ausgebucht. Gleichzeitig melden sich täglich weitere Unternehmen als Teilnehmer der Initiative an.

Breite Unterstützung

Die Mitglieder sind Unternehmen unterschiedlichster Größen und aus diversen Branchen. Hieraus wird deutlich, dass inzwischen nicht nur IT-Unternehmen, sondern auch Organisationen aus anderen Wirtschaftszweigen die Notwendigkeit von IT-Sicherheit erkannt haben. Unter anderem diese Entwicklung führte letztendlich dazu, dass nach Gründung der Allianz für Cyber-Sicherheit ein Beirat ins Leben gerufen wurde. Hier beraten die Vorsitzenden der deutschen Spitzenverbände

- Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI),
- Bundesverband der Deutschen Industrie (BDI),
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM),
- Deutscher Industrie- und Handelskammertag (DIHK),
- Gesellschaft für Informatik e. V. (GI),
- Verband Deutscher Maschinen- und Anlagenbau (VDMA) und
- VOICE – Verband der IT-Anwender

gemeinsam mit dem Bundesministerium des Inneren (BMI) und dem BSI über die zukünftige Ausrichtung der Initiative und Möglichkeiten, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen weiter zu stärken und die IT-Sicherheitskompetenz in den einzelnen Branchen auszubauen.

Ausblick

Das Interesse an Cyber-Sicherheits-Themen ist gerade bei kleinen und mittelständischen Unternehmen hoch. Nicht zuletzt aufgrund immer neuer Angriffe, die sich in den täglichen Nachrichten wiederfinden – bspw. der Angriff auf den deutschen Bundestag oder verschiedene Ransomware-Wellen, wie „WannaCry" – wird die Allianz für Cyber-Sicherheit voraussichtlich auch in den nächsten Jahren weiter wachsen. Bereits jetzt werden die Weichen gestellt, um noch mehr Interessenten bedienen zu können: Cyber-Sicherheits-Tage werden in Zukunft planmäßig nicht nur alle drei, sondern alle zwei Monate organisiert. Außerdem ist eine Stärkung der Medienarbeit in Planung, um auch auf diesem Weg die im Kontext der Allianz für Cyber-Sicherheit erarbeiteten Informationen weiter verbreiten zu können.

Gleichzeitig lassen sich mit einer derart großen Teilnehmerbasis auch verschiedene Vorhaben realisieren: So führt die Allianz für Cyber-Sicherheit jährlich die Cyber-Sicherheits-Umfrage durch, in der deutsche Institutionen zu ihrer Betroffenheit durch Cyber-Angriffe befragt werden (siehe Infokasten). Außerdem wurde auf der Allianz-Website eine Meldestelle eingerichtet: Hier können deutsche Unternehmen freiwillig und anonym

über IT-Sicherheitsvorfälle berichten. Die regelmäßig eingehenden Hinweise gehen in den BSI-Lagebericht ein und helfen, einen realistischen Eindruck von der aktuellen Cyber-Bedrohungslage zu erhalten. Hier sind auch in den kommenden Monaten weitere Aktivitäten geplant.

Vor fünf Jahren konnte mit der Gründung der Allianz für Cyber-Sicherheit eine solide Basis geschaffen werden, um das Thema Cyber-Sicherheit in der deutschen Wirtschaft zu verankern. Im Rahmen der it-sa werden sie sich dann – wie jedes Jahr – in Nürnberg treffen: die Teilnehmer und Partner für Gespräche in den Messehallen, der Beirat zum Schmieden weiterer Pläne für die Zukunft und nicht zuletzt bei der offiziellen Geburtstagsfeier mit Reden von Vertretern aus Politik und Verbänden sowie Erfahrungsberichten der Mitglieder und einem gemeinsamen Blick in die Zukunft. Die immer weiter wachsende Reichweite der Allianz für Cyber-Sicherheit und die immer neuen Bedrohungen aus dem Cyber-Raum lassen erahnen, dass die Initiative weiterhin einen wichtigen Beitrag bei der Stärkung des Themas Cyber-Sicherheit am Standort Deutschland leisten wird. ■

Kontaktdaten

Geschäftsstelle Allianz für Cyber-Sicherheit
Bundesamt für Sicherheit in der Informationstechnik
Telefon: 0800 2741000
E-Mail: info@cyber-allianz.de

Web-Adressen
www.allianz-fuer-cybersicherheit.de
www.allianz-fuer-cybersicherheit.de/ACS/Meldestelle
www.cyber-sicherheits-umfrage.de
www.bsi.bund.de/Lagebericht

kurz notiert

Impulse für eine smarte und sichere digitale Gesellschaft

87 % der Bevölkerung in Deutschland halten Sicherheit im Internet für wichtig, doch weniger als die Hälfte kennt sich damit aus – das ist ein Ergebnis einer repräsentativen Bevölkerungsumfrage, die das BSI in Auftrag gegeben hat. Die Ergebnisse der Umfrage und zahlreiche Experteninterviews dienten als Grundlage für ein Impulspapier, das im Rahmen des BSI-Projekts „Digitale Gesellschaft: smart & sicher“ von Vertretern der Zivilgesellschaft, Kultur, Wirtschaft, Wissenschaft und Verwaltung entwickelt und Anfang September in Berlin vorgestellt wurde.

„Informationssicherheit ist ein gesamtgesellschaftliches Thema, für das wir mit dem Projekt ‚Digitale Gesellschaft: smart & sicher‘ den notwendigen gesamtgesellschaftlichen Diskurs mit angestoßen haben. Zahlreiche Impulse, die von den Akteuren heute vorgestellt wurden, wie etwa das Prinzip ‚Security by Design und by Default‘ oder das IT-Gütesiegel, decken sich mit Ansätzen des BSI für mehr Sicherheit im Cyber-Raum. Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung, daher werden wir als nationale Cyber-Sicherheitsbehörde den Dialog fortführen und intensivieren, um gemeinsam weitere Lösungsansätze für die smarte und sichere Gesellschaft zu entwickeln“, so BSI-Präsident Arne Schönbohm.

Ziel des Impulspapiers ist, den aktuellen Stand der gesellschaftlichen Debatte zu Fragen einer sicheren Informationsgesellschaft transparent zu machen und den weiteren Diskurs anzuregen. Insbesondere werden die Punkte der staatlichen und gesamtgesellschaftlichen Verantwortung, Bildung und Forschung, Haftung, Sicherheitsstandards sowie Zertifizierung adressiert.

Zwei Drittel der Bevölkerung nannten Sicherheitstests, Sicherheitsrichtlinien und klare Haftungsregelungen als Beitrag zu mehr Sicherheit im Cyber-Raum. Die in Interviews befragten Experten für IT-Sicherheit sprachen sich für eine Kennzeichnung von internetfähigen Produkten bezüglich ihrer Informationssicherheit aus. Für entsprechende Anforderungen einer Kennzeichnung sollten ihrer Meinung nach das BSI und ein heterogen zusammengesetztes Experten-Gremium zuständig sein. Auch effektive Haftungsregelungen als Anreiz zur Steigerung der IT-Sicherheit wurden von den Expertinnen und Experten identifiziert und diskutiert. Die vollständige Broschüre mit allen Ergebnissen ist über die Projektseite www.bsi.bund.de/susi/ kostenlos abrufbar. Eine ausführliche Betrachtung der Ergebnisse folgt darüber hinaus auch im nächsten BSI-Forum. ■

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 Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware)	Smartcard-Controller	EAL 6+ BSI-DSZ-CC-0951-V2-2017 2017-07-26
NXP Semiconductors Germany GmbH	NXP Secure Smart Card Controller N7021 VA including IC Dedicated Software	Smartcard-Controller	EAL 6+ BSI-DSZ-CC-0977-2017 2017-07-24
IBM Corporation	IBM z/OS, Version 2 Release 2	Betriebssystem	EAL 4+ BSI-DSZ-CC-0948-2017 2017-07-10
Infineon Technologies AG	IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated firmware	Smartcard-Controller	EAL 6+ BSI-DSZ-CC-0945-2017 2017-07-10
Infineon Technologies AG	IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware	Smartcard-Controller	EAL 6+ BSI-DSZ-CC-0961-2017 2017-07-10
Atos IT Solutions and Services GmbH	CardOS V5.3 QES, V1.0	Smartcard-Controller	BSI-DSZ-CC-0921-2014-MA-01 2017-07-07
Atos IT Solutions and Services GmbH	CardOS V5.0 with Application for QES, V1.0	Smartcard-Controller	BSI-DSZ-CC-0833-2013-MA-01 2017-07-07
Dell Inc.	Dell EqualLogic PS 4000 Series Storage Firmware v7.1.1	Storage-Area-Network	EAL 2+ BSI-DSZ-CC-1008-2017 2017-06-12

Anmerkung:

– Die zugehörigen Zertifizierungsreporte mit Zertifikaten sind auf der Webseite 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
secunet Security Networks AG	secunet(konnektor v2.0	Konnektor	BSI-DSZ-CC-1044

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 bestätigte Produkte gemäß Signaturgesetz (SigG)

Hersteller	Produktbezeichnung	Produkttyp	Registriernummer
T-Systems International GmbH	TCOS Residence Permit Card Version 1.0, Release 1/SLE78CLX1440P und TCOS Residence Permit Card Version 1.0, Release 2/SLE78CLX1440P	Sichere Signaturerstellungs-einheit	2. Nachtrag zur Bestätigung BSI.02131.TE.08.2011 2017-06-23

4. Vom BSI zertifizierte und registrierte Schutzprofile

Entwickler	Profilbezeichnung	ID Ausstellungsdatum	gültig bis
Bundesamt für Sicherheit in der Informationstechnik	FIDO Universal Second Factor (U2F), Version 1.0	BSI-CC-PP-0096-2017 2017-07-05	2027-07-04
Bundesamt für Sicherheit in der Informationstechnik	Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP) – Schutzprofil für das Sicherheitsmodul des Smart Meter Mini-HSM, V1.0	BSI-CC-PP-0095-2017 2017-06-29	2027-06-26

5. Vom BSI erteilte Standortzertifikate

Antragsteller	Entwicklungs-/ Produktionsstandorte	ID Ausstellungsdatum	gültig bis
King Yuan Electronics Co., Ltd (KYEC)	King Yuan Electronics Co., Ltd., Chu-Nan Factory	BSI-DSZ-CC-S-0088-2017 2017-06-26	2018-10-19

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

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0286-2017	WOLFF Daten. Menschen. Marketing.	Der Informationsverbund am Standort Berlin umfasst die gesamte interne Organisation mit der Verwaltung, der Lohn- & Finanzbuchhaltung, dem Bereich Kommunikation & Vertrieb und der IT-Administration. Darüber hinaus die Erstellung von Marketing-Analysen und -Konzepten, das operative Kundendatenmanagement sowie das Management von Hosting und Betrieb individuell realisierter Portal-Lösungen. Ausgenommen ist die reine Software-Entwicklung und vereinzelte Bestandsprojekte, die historisch bedingt nicht die ISO-27001-Standards erfüllen und nicht modifiziert wurden/werden sollten.	2020-07-09
BSI-IGZ-0281-2017	GkD – Gesellschaft für kommunale Dienstleistungen mbH	Der Informationsverbund „GkD“ stellt höchstverfügbare IT-Infrastruktur an zwei Rechenzentrumsstandorten in Köln bereit. Räumlich besteht der Verbund aus den beiden RZ und den Büroräumen der GkD. Die Kerntätigkeiten sind Hosting und Administration von Anwendungen und Daten diverser Kunden, mit Schwerpunkt auf Versorgungsunternehmen. Organisatorisch besteht die GkD aus den Einheiten Change, Computing, Desktop, Helpdesk und Network und stellt über eine moderne IT-Infrastruktur hinaus auch die damit verbundenen Dienstleistungen inklusive der für diese Dienstleistungen erforderlichen technischen Systeme bereit. Zentrale kaufmännische Bereiche wie Personal und Abrechnung wurden ausgelagert und sind nicht Teil des Informationsverbunds.	2020-06-25
BSI-IGZ-0276-2017	HiSolutions AG	Der lnformationsverbund unterstützt die Geschäftsprozesse zur Erbringung der Beratungsdienstleistungen durch die HiSolutions AG. Technische Infrastruktur: Zur Erbringung der Beratungsleistungen benötigt die HiSolutions AG unterschiedlichste Anwendungen und IT-Systeme. lm Rahmen der Beratungstätigkeit werden Notebooks verwendet, mit denen bei einem mobilen Einsatz beim Kunden vor Ort die Einwahl über eine VPN-Verbindung in das Firmennetz erfolgen kann. Für die Bürokommunikation wurde eine E-Mail-Infrastruktur mit Integration von mobilen Geräten implementiert. Über die mobilen Geräte erfolgt die Sprach- und E-Mail-Kommunikation. Zusätzlich wird eine Sprachkommunikation über eine zentrale Telefonanlage angeboten. Im Rahmen der Projekttätigkeiten wird auf Anwendungen zugegriffen, die auf Serversystemen betrieben werden, welche sich in einem gesicherten Serverraum der HiSolutions AG befinden. Die bereitgestellten Serversysteme werden zum Teil in einer Virtualisierungsinfrastruktur abgebildet. Entsprechend der Funktionalität und des Schutzbedarfs erfolgt eine Aufteilung der Systeme in unterschiedliche Netze, welche durch Sicherheitssysteme geschützt werden.	2020-05-31