Im Birkenfeld 1a
65779 Kelkheim, Germany

Web Site: *www.isaca.de*
E-mail: *info@isaca.de*

Trust in, and value from, information systems
Germany Chapter

Abs.: ISACA Germany Chapter e.V. Im Birkenfeld 1a, 65779 Kelkheim

Bundesministerium des Innern
Referat IT
Berlin

Frankfurt, 3.4.2013

Stellungnahme zum Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Der ISACA Germany Chapter e.V. ist mit über 2.300 Mitgliedern als eingetragener Verein Teil des internationalen Verbandes ISACA, dem weltweit mehr als 100.000 Know-how-Träger in über 180 Ländern der Welt angehören. Wir fördern die Anerkennung des Berufstandes durch die Verbreitung von Berufsstandards und Arbeitstechniken sowie durch die ständige Weiterbildung und die international anerkannten Zertifizierungen Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT) und Certified in Risk and Information System Control (CRISC).

Ausgangspunkt

Die Gewährleistung von Cyber-Sicherheit gehört zu den zentralen Herausforderungen unserer Zeit. Wesentliche nationale und internationale IT-Ausfälle werden zunehmend als reale Gefahr und globale Bedrohung angesehen.

Bundesinnenminister Dr. Friedrich hat daher die Initiative ergriffen und einen Gesetzesentwurf zur Verbesserung der IT-Sicherheit kritischer Infrastrukturen vorgelegt. Der Entwurf befindet sich in der Abstimmung zwischen den Ministerien und wurde am 5. März 2013 den betroffenen Verbänden zur Stellungnahme zugeleitet. Bedauerlicherweise wurde das ISACA Germany Chapter e.V. nicht wie üblich angeschrieben. Der Verband hat sich aufgrund der Kritikalität und der Wichtigkeit dieses Themas dennoch entschlossen, den Referentenentwurf, der vom Bundesministerium des Innern auf der Webseite http://www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html zur Verfügung gestellt wird, zu kommentieren.

Ein Großteil der Geschäftsprozesse am Wirtschaftsstandort Deutschland stützt sich auf die Informationstechnologie. Der ISACA Germany Chapter e.V. hält es daher für unumgänglich, die Prozesse und die zugrundeliegende Informationstechnologie widerstandsfähiger gegen die Vielzahl von Cyber-Bedrohungen zu machen. Aufgrund der Praxiserfahrungen unserer Mitglieder, der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten in Deutschland unterstützt der

Verein den Ansatz der Bundesregierung nachdrücklich. Es gilt, das hohe Niveau im Hinblick auf die Informationssicherheitsgrundwerte Verfügbarkeit, Vertraulichkeit und Integrität aufrecht zu halten und zu stärken, um so für Deutschland weiterhin die bestehenden Standortvorteile zu bewahren und auszubauen.

Der ISACA Germany Chapter e.V. unterstützt das Ziel, einheitliche Sicherheitslevels bei unterschiedlichen Betreibern kritischer Infrastrukturen zu etablieren und hält eine intensive Zusammenarbeit von Staat und Wirtschaft in den nachfolgenden Punkten für geboten:

- Aufbau von fachlicher Expertise in der Informationssicherheit
- Gegenseitiger vertrauensvoller Erfahrungsaustausch zwischen den am Wirtschaftsstandort Deutschland tätigen privaten und staatlichen Stellen, insbesondere im Hinblick auf Angriffe und Spionage
- Stärkung der Strafverfolgungsbehörden, um Cyber-Kriminalität angemessen entgegentreten zu können
- Etablierung von präventiven und reaktiven Maßnahmen gegen bekannte IT-Sicherheitsvorfälle
- Aufbau einer zentralen Cyber-Crime-Notfall-Meldestelle
- Aufbau eines Cyber-Security-Abwehrzentrums, um zeitnah auf gezielte „Fire-Sale[1]“- Angriffe reagieren zu können

Damit dieser Gesetzesentwurf seine Wirkung entfalten kann, ist es nach Auffassung des ISACA Germany Chapter e.V. notwendig, eine breite Zustimmung zu erhalten. Ferner sollten die schon vorhandenen Sicherheitsbestrebungen in der Wirtschaft gewürdigt werden.

Der ISACA Germany Chapter e.V. erlaubt sich, vor diesem Hintergrund den Gesetzesentwurf nachfolgend zu kommentieren und hofft somit seinen Beitrag leisten zu können, um dieses wichtige Vorhaben zu unterstützen:

Zu Artikel 1
(Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik)

(1)

Der ISACA Germany Chapter e.V. hält den Ansatz, sektorspezifischen Schutz für Betreiber kritischer Infrastrukturen umsetzen zu wollen, für einen angemessenen Weg. Die Definition, welche Bereiche zu den Betreibern kritischer Infrastrukturen (KRITIS) gehören, sollte jedoch - aus unserer Erfahrung als Prüfer in fast allen Branchen in Deutschland - wesentlich konkreter ausgeführt werden.

Wir schlagen daher vor, auf Basis der Erfahrungswerte des BSI, vor einer Anhörung des BMI gemäß §10 Absatz 1 detaillierte Kriterien zu definieren, welche Organisationsformen bzw. Unternehmensarten und welche Bereiche sich diesem Gesetz unterzuordnen haben, bzw. der Meldepflicht unterliegen. Lediglich die Kategorisierung als KRITIS-Unternehmen lässt bereits heute vielen Organisationen mannigfache Möglichkeiten und Spielräume, sich dem Gesetz bzw. dessen effektiver Umsetzung zu entziehen, und es ist mit erheblichem Widerstand seitens der Betroffenen zu rechnen.

[1] Ziel des Angreifers bei einem Fire-Sale ist es, die kritische Infrastruktur des Landes unter Kontrolle zu bekommen und mit gezielten Angriffen diese vollständig zum Erliegen zu bringen.

(2)

Das BSI wird hier als beratende Stelle für die Unterstützung für Betreiber kritischer Infrastruktur alleinig genannt. Der Verband sieht das Wahlrecht der Betreiber beschnitten, zumal hier die Gefahr des Eingriffs in den funktionierenden, privatwirtschaftlichen Beratungsmarkt besteht.

Wir empfehlen daher, stattdessen das bestehende BSI-Programm „Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern", um Beratungsleistungen zu erweitern. Dazu müssen aus unserer Sicht u. a. auch die durch die ISACA am Markt etablierten Standards, Prüfprogramme und Frameworks zählen. Aus diesem Grund sollte der letzte Satz § 3 Abs. 3 wie folgt erweitert werden:

„Das Bundesamt kann (…) beraten und unterstützen. Die Beratung und Unterstützung kann ebenfalls durch qualifizierte Dienstleister, die eine nachweisbare Qualifikation im Informationssicherheitsumfeld nach dem aktuellen Stand der Technik (beispielsweise nach ISO/IEC 27001, IT-Grundschutz, COBIT 5, OSSTMM, OWASP, etc.) besitzen, erfolgen."

(3)

Die Formulierung, dass angemessene Maßnahmen zu treffen sind kann dahingehend interpretiert werden, dass deren Planung allein auch schon ausreichend anzusehen ist, obwohl deren Umsetzung möglicherweise weit hinter den veranschlagten zwei Jahren liegt.

Zur Klarstellung dieses Sachverhalts sollte auch auf die Umsetzung verwiesen werden und der erste Satz von § 8a Abs. 1 wie folgt erweitert werden:

„Betreiber kritischer Infrastrukturen sind verpflichtet, binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen und umzusetzen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind."

(4)

Der Begriff der „Angemessenheit" wird nur soweit definiert, dass der erforderliche Aufwand „nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur" stehen soll. Damit kann die Angemessenheit einzelner Maßnahmen ggf. ausschließlich von allgemeinen oder individuellen Wirtschaftlichkeitserwägungen abhängig gemacht werden.

Damit eine Maßnahme nicht ausschließlich mit Blick auf ihre Wirtschaftlichkeit oder eine einfache Risikoübernahmeerklärung unterlassen werden kann, sollte im Gesetz ergänzend gefordert werden, dass die Beurteilung der Angemessenheit durch begründete und dokumentierte Risikobewertungen zu erfolgen hat. Diese Risikobewertungen müssen auf Basis qualitativer und quantitativer Kriterien durchgeführt werden, so dass im Ergebnis eine objektive und nachvollziehbare Analyse des möglichen Schadens bzw. der möglichen Auswirkungen sowie der Eintrittswahrscheinlichkeit vorgelegt werden kann. Aus diesem Grund sollte der § 8a Abs. 1 wie folgt erweitert werden:

„(..) Organisatorische und technische Vorkehrungen und sonstige Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den auf Basis einer objektiven und nachvollziehbaren Risikoanalyse ermittelten möglichen Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht."

(5)

Die im Rahmen des Gesetzes geforderte Meldepflicht von Sicherheitsvorfällen nach § 8b Abs. 4 und die Übermittlung weiterer Informationen (z.B. nach § 8a Abs. 4 die Übermittlung von Aufstellungen durchgeführter Sicherheitsaudits) an die zentrale Meldestelle führt zu der Tatsache, dass die Meldestelle selbst und der gesamte Datenaustausch dorthin und von dort besonderen Sicherheitsanforderungen unterliegt.

Es ist daher sicherzustellen und im Gesetzestext verbindlich zu verankern, dass sowohl die Übermittlung von Informationen zur zentralen Meldestelle als auch die Übermittlung und Verteilung von Informationen von der Meldestelle hin zu den Betreibern kritischer Infrastrukturen auf eine ausreichend sichere Art und Weise erfolgen muss. Der Schutz der Vertraulichkeit und der Integrität der übermittelten sensiblen Daten und Informationen muss zu jedem Zeitpunkt sichergestellt sein.

(6)

Der Verein unterstützt ausdrücklich die Einrichtung des BSI als zentrale Meldestelle für Cyber-Sicherheit in Deutschland gemäß § 8b Absatz 1. Aus unserer Sicht ist die kurzfristige Bereitstellung konsolidierter Informationen zum Sicherheitslagebild ein Mehrwert.

Wir empfehlen hier ergänzend zu den Meldungen von Betreibern kritischer Infrastrukturen die Einbeziehung weiterer staatlichen Sicherheitsorgane sowie privatwirtschaftlichen CERTs und sonstige Meldungen zu Cyber-Sicherheitsvorfällen. Das Meldeverfahren der Allianz für Cybersicherheit kann hier als Beispiel dienen. Wir weisen darauf hin, dass es zu einer personellen und Sachmittelaufstockung beim BSI kommen sollte, damit es die Aufgaben (Rolle als Informationssenke und Informationsquelle) angemessen bewältigen kann.

(7)

Der Gesetzentwurf verweist in § 8a Abs. 4 auf angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz informationstechnischer Systeme, Komponenten oder Prozesse, die mindestens alle zwei Jahre durch anerkannte Sicherheits-Auditoren überprüft werden sollen.

Wir empfehlen dringend eine Klarstellung, in welche Tiefe, mit welchem Detaillierungsgrad und gegen welche (Prüf-)Standards die geforderten Audits durchgeführt werden müssen. Eine ergänzende Beschreibung erscheint hier sinnvoll. Aufgrund der sehr individuellen Ausprägung der IT-Umgebung bei den einzelnen Branchen und Betreibern kritischer Infrastrukturen empfehlen wir, branchenübergreifende und bereits etablierte und anerkannte „Best-Practice“- Standards und Frameworks (beispielsweise ISO/IEC 27001, COBIT) als Bewertungsgrundlage zu nehmen und um sektorspezifische Anforderungen (beispielsweise § 109 TKG, Anlage (zu § 9 Satz 1) BDSG, AT 4.3 ff. und BT 2 ff. MaRisk (BA), PCI DSS) zu ergänzen.

(8)

Mit Blick auf die Kontrolle durch anerkannte Auditoren ist klarzustellen, dass Audits nur von qualifiziertem Fachpersonal durchgeführt werden dürfen.

Wir empfehlen, die auf dem Markt einschlägigen Auditoren-Qualifikationen (beispielsweise ISO 27001 Lead Auditoren, CISA) anzuerkennen. Eine mögliche Ergänzung zu § 8a Abs. 4 wäre:

"Diese Sicherheitsaudits sollen von Auditoren mit vom BSI akkreditierter Qualifikation (beispielsweise ISO 27001 Lead Auditoren oder Certified Information Systems Auditoren) sowie mit

notwendigem branchenspezifischen Know-how durchgeführt werden. Die Prüfung muss die Mindeststandards in der Informationssicherheit und, in Ergänzung dazu, die jeweiligen branchenspezifischen Standards zum Schutz der kritischen Infrastruktur und der wesentlichen informationstechnischen Systeme, Komponenten, Prozesse und Dienstleister beinhalten."

Zu Artikel 2
(Änderung des Bundeskriminalamtgesetzes)

Es sind beabsichtigte Änderungen von § 4 des Bundeskriminalamtgesetzes aufgeführt. Leider ist an keiner weiterer Stelle des Referentenentwurfs erkennbar, ob und von wem das BKA hinzugezogen wird bzw. welche Instanz beurteilt, ob z. B. ein an die zentrale Meldestelle gemeldetes Ereignis den Straftatbestand erfüllt und ob sich daraus dann ergibt, dass das BKA Ermittlungen aufnimmt bzw. was die zugrundeliegenden Rahmenbedingungen sind.

Es sollte daher erreicht werden, dass den bei der Umsetzung des Gesetzes involvierten Stellen und den Betreibern von kritischen Infrastrukturen die Zusammenhänge transparent gemacht werden und Rahmenbedingungen klar beschrieben sind.

Zur Begründung

A: Allgemeiner Teil

Teil III (Erfüllungsaufwand)

Die durch die geforderten Audits entstehenden Mehraufwände können darüber hinaus eine wesentliche Mehrbelastung darstellen. Es sollten deshalb, wie schon zuvor erwähnt, die einzuhaltenden Standards (beispielsweise ISO/IEC 27001) definiert werden.
Darüber hinaus müssen die Aufwände für die geforderten Audits und die interne Organisation für Warn- und Alarmierungskontakte berücksichtigt werden.

Die Fachgruppe Informationssicherheit des ISACA Germany Chapter e.V. entwickelt derzeit z. B. im Rahmen der Allianz für Cybersicherheit gemeinsam mit dem BSI einen Prüfleitfaden für eine branchenübergreifende Cyber-Sicherheitsrevision.
Das ISACA Germany Chapter e.V. bietet darüber hinaus an, bei seinen Mitgliedern eine Umfrage durchzuführen, um die zu erwartenden Aufwände abschätzen zu können.

Zweiter Teil: Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Nummer 4 (§ 8a Sicherheit der Informationstechnik kritischer Infrastrukturen)

In der Begründung zum Gesetzentwurf wird dargestellt: „Eine Ausgestaltung der Sicherheitsaudits soll nicht im Detail gesetzlich vorgesehen werden …. Eine Kontrolle der Einhaltung der Erfordernisse nach Absatz 1 kann zudem über etablierte Prüfmechanismen erfolgen. So prüfen Wirtschaftsprüfer bereits jetzt die im Rahmen der Jahresabschlussprüfung rechtsrelevanten IT-Systeme."

Das ISACA Germany Chapter e.V. weist ausdrücklich drauf hin, dass Wirtschaftsprüfer im Rahmen der Jahresabschlussprüfung IT-Systeme nur im Hinblick auf die Ordnungsmäßigkeit und Sicherheit der Rechungslegung gemäß den einschlägigen rechtlichen Grundlagen (HGB, AO, GoBS usw.)

sowie nach den hieraus abgeleiteten Standards des Instituts der Wirtschaftsprüfer (IDW) prüfen. Diese berücksichtigen nicht explizit die Prüfung kritischer Infrastrukturen im Sinne der nationalen Cyber-Sicherheit. Die im Gesetzentwurf vorgesehene Sicherheitsauditierung muss sich aus Sicht des Vereins jedoch auf die operative Vertraulichkeit, Integrität und Verfügbarkeit der Informationsverarbeitung beziehen und erfordert daher eine entsprechende Qualifikation des Prüfers.

Wir empfehlen daher dringend den Satz „So prüfen Wirtschaftsprüfer bereits jetzt die im Rahmen der Jahresabschlussprüfung rechtsrelevanten IT-Systeme.“ zu löschen, da dies zu Missverständnissen bei den betroffenen Unternehmen führen kann. Stattdessen empfehlen wir, die Formulierung wie folgt zu ändern:

„Ein Sicherheitsaudit kann auf die Ergebnisse weiterer Prüfungen (beispielsweise Zertifizierungen nach ISO/IEC 27001) zurückgreifen, sofern sich diese auf die kritischen Infrastrukturen beziehen. Die Prüfer sollten einschlägige Qualifikationen (beispielsweise ISO 27001 Lead Auditor oder CISA) nachweisen und über branchenspezifische Erfahrungen im Bereich der zu prüfenden kritischen Infrastruktur verfügen.

Andreas Teuscher
(Vizepräsident - Fachgruppen/Arbeitskreise)

Stefan Wittjen
(Vizepräsident - Finanzen/Verwaltung)