Cyber-Sicherheits-Check

Matthias Becker

Bundesamt für Sicherheit in der Informationstechnik
matthias.becker@bsi.bund.de

Zusammenfassung

Mit dem in Kooperation zwischen der Allianz für Cyber-Sicherheit (ACS) im Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem ISACA Germany Chapter [ISACA] entwickelten Cyber-Sicherheits-Check werden Institutionen in die Lage versetzt, schnell den Status ihrer Cyber-Sicherheit auf Basis ihrer Cyber-Sicherheits-Exposition [ACS1] zu bestimmen und somit aktuellen Bedrohungen aus dem Cyber-Raum wirksam zu begegnen. Grundlage eines jeden Cyber-Sicherheits-Checks sind die vom BSI veröffentlichten Basismaßnahmen der Cyber-Sicherheit [ACS2]. Der Leitfaden Cyber-Sicherheits-Check liefert konkrete Vorgaben und Hinweise für die Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden und die Berichtserstellung. IT-Sicherheitsbeauftragten, Revisoren und sonstigen Verantwortlichen für die Informationssicherheit dient der Leitfaden insbesondere dazu, sich einen Überblick über das Thema Cyber-Sicherheit zu verschaffen, die zu beurteilenden Sicherheitsaspekte zu betrachten und sich mit dem Ablauf eines Cyber-Sicherheits-Checks vertraut zu machen.

1 Einführung in die Cyber-Sicherheit

Cyber-Sicherheit, Cyber-Angriff, Cyber-Kriminalität und Cyber-Kriegsführung sind längst zu Schlagwörtern in Sicherheitsdiskussionen avanciert. Das ist zum Teil der technischen Entwicklung geschuldet, liegt im Wesentlichen aber an der stetig steigenden Zahl von Sicherheitsvorfällen, kriminellen Handlungen und neuartigen informationsbasierten Angriffsmethoden. Der Mythos, dass es sich hierbei um Aktivitäten von Einzelnen mit einem Ausnahmewissen handelt, ist der Erkenntnis gewichen, dass Cyber-Sicherheit eine wichtige Facette der Sicherheit ist und diese durch die Leitung / das Management einer Institution berücksichtigt werden muss. Sie erfordert den Einsatz angemessener Ressourcen und sollte fester Bestandteil des unternehmerischen Risikomanagements sein.

Der vorliegende Leitfaden und die zugrunde liegenden Maßnahmenziele für die Beurteilung wurden so konzipiert, dass APT-basierte Cyber-Angriffe grundsätzlich erschwert und die Fähigkeiten zur Entdeckung eines Angriffs und zur adäquaten Reaktion gestärkt werden. Das Risiko, einem APT-basierten Cyber-Angriff zum Opfer zu fallen, kann somit bei regelmäßiger Durchführung von Cyber-Sicherheits-Checks minimiert werden. Sofern eine Institution bereits Opfer eines APT-Angriffs wurde bzw. der Verdacht auf einen APT-Angriff besteht, können dem BSI-Dokument „Erste-Hilfe bei einem APT-Angriff“ [ACS3] konkrete Maßnahmen zur Reaktion entnommen werden.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 227-235.

2 Rahmenbedingungen

2.1 Cyber-Sicherheitsstrategie für Deutschland

Ziel der im Februar 2011 vom Bundeskabinett beschlossenen Cyber-Sicherheitsstrategie für Deutschland [BMI1] ist es, Cyber-Sicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen. Erforderlich ist ein eng verzahntes Vorgehen aller Akteure in Staat, Wirtschaft und Forschung. Die Strategie bündelt die Aktivitäten aller Bundesministerien.

IT-Angriffe auf lebenswichtige Infrastrukturen stellen eine besondere Bedrohung dar. Kernpunkte der Strategie sind daher der verstärkte Schutz sogenannter Kritischer Infrastrukturen vor IT-Angriffen, der Schutz der IT-Systeme in Deutschland, der Aufbau eines nationalen Cyber-Abwehrzentrums sowie die Einrichtung eines nationalen Cyber-Sicherheitsrates.

Daneben forciert die nationale Cyber-Sicherheits-Strategie, die vorrangig auf präventive und reaktive Schutzmaßnahmen setzt, die Stärkung der IT-Sicherheit in der öffentlichen Verwaltung, den Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie, die wirksame Kriminalitätsbekämpfung auch im Cyber-Raum sowie ein effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit.

Das BMI koordiniert die Umsetzung über die Bundesbeauftragte für Informationstechnik, Staatssekretärin Cornelia Rogall-Grothe. Sie ist Vorsitzende des Cyber-Sicherheitsrates, in dem wesentliche Leitlinien und Ziele der nationalen Cyber-Sicherheitsstrategie festgelegt werden. Dazu gehört die Personalentwicklung der Bundesbehörden ebenso wie das gesamtstaatliche Instrumentarium zur Abwehr von Cyber-Angriffen.

2.2 Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit [ACS] ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Derzeit beteiligen sich nahezu 798 teilnehmende Institutionen, über 77 aktive Partner und mehr als 29 Multiplikatoren an der Allianz.

Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Zur gemeinsamen Förderung der Cyber-Sicherheit arbeitet das BSI dabei im Rahmen der Allianz intensiv mit Partnern und Multiplikatoren zusammen.

Zur Erreichung dieser Ziele verfolgt die Allianz u.a. diese Maßnahmen:

- Erstellung und Pflege eines aktuellen Lagebilds
- Bereitstellung von Hintergrundinformationen und Lösungshinweisen
- Intensivierung des Erfahrungsaustausches zum Thema Cyber-Sicherheit
- Ausbau von IT-Sicherheitskompetenz in Organisationen mit intensivem IT-Einsatz

Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis auf und initiiert und betreibt Erfahrungs- sowie Expertenkreise zur Cyber-Sicherheit. Ergänzt werden diese Angebote durch weitere Beiträge der Partner – z.B. in Form von Schulungen, zusätzlichen Informationsveranstaltungen oder kostenlosen Bereitstellung von Sicherheitsprodukten.

3 Der Cyber-Sicherheits-Check

3.1 Ziele und Zielgruppen des Cyber-Sicherheits-Checks

Die Bedrohungen aus dem Cyber-Raum sind real. Um Cyber-Angriffen wirksam zu begegnen, ist eine intensive Kooperation von Staat, Wirtschaft und Verbänden erforderlich. Es gilt, vorhandenes Wissen zu bündeln, um angesichts neuer Angriffsszenarien vorbereitet zu sein. Aus diesem Grund haben sich das Bundesamt für Sicherheit in der Informationstechnik und das ISACA Germany Chapter e.V. dazu entschlossen, in Kooperation eine praxisorientierte Vorgehensweise zur Beurteilung der Cyber-Sicherheit in Unternehmen und Behörden zu entwickeln. Der Cyber-Sicherheits-Check hilft dabei, den Status der Cyber-Sicherheit auf Basis der Cyber-Sicherheits-Exposition (siehe [ACS2]) zu bestimmen und somit aktuellen Bedrohungen aus dem Cyber-Raum wirksam zu begegnen. Grundlage eines jeden Cyber-Sicherheits-Checks sind die vom BSI veröffentlichten Basismaßnahmen der Cyber-Sicherheit (siehe [ACS3]).

3.2 Kooperation BSI / ISACA

Der Leitfaden Cyber-Sicherheits-Check wurde durch die Fachgruppe Informationssicherheit des ISACA Germany Chapter e.V. gemeinsam mit Experten des BSI entwickelt. Durch diesen aktiven Partnerbeitrag dokumentiert das ISACA Germany Chapter e.V., dass es die Ziele der Allianz für Cyber-Sicherheit mit seinem guten Namen, den ihm zur Verfügung stehenden Mitteln und dem Fachwissen seiner Mitglieder unterstützt.

3.3 Grundsätze des Cyber-Sicherheits-Checks

Der vorliegende Leitfaden und die zugrunde liegenden Maßnahmenziele für die Beurteilung wurden so konzipiert, dass das Risiko, einem Cyber-Angriff zum Opfer zu fallen, bei regelmäßiger Durchführung von Cyber-Sicherheits-Checks minimiert werden kann.

Um Vertrauen in eine objektive Beurteilung zu schaffen, müssen folgende Voraussetzungen sowohl durch Einzelpersonen als auch durch Unternehmen, die Dienstleistungen im Bereich der Cyber-Sicherheit erbringen, eingehalten werden:

- Eine formale Beauftragung des Cyber-Sicherheits-Checks durch die Institution (siehe dazu ISACA IT-Prüfungsstandard 1001 – AuditCharter)
- Unabhängigkeit (siehe dazu ISACA IT-Prüfungsstandard 1002 – Organisatorische Unabhängigkeit und 1004 – Persönliche Unabhängigkeit)
- Rechtschaffenheit und Vertraulichkeit (siehe dazu ISACA IT-Prüfungsstandard 1005 – Berufsübliche Sorgfalt)
- Fachkompetenz (siehe dazu ISACA IT-Prüfungsstandard 1006 – Expertise)
- Nachweise und Nachvollziehbarkeit (siehe dazu ISACA IT-Prüfungsstandard 1205 – Nachweise)
- Objektivität und Sorgfalt (siehe dazu ISACA IT-Prüfungsstandards 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen und 1204 – Wesentlichkeit)

- Sachliche Darstellung (siehe dazu ISACA IT-Prüfungsstandard 1401 – Berichterstattung)

Grundvoraussetzung für jede Beurteilung im Rahmen des Cyber-Sicherheits-Checks ist ein uneingeschränktes Informations- und Einsichtnahmerecht. Dies bedeutet, dass dem Beurteiler keine Informationen vorenthalten werden dürfen. Hierzu gehört auch die Einsichtnahme in sensible oder amtlich geheim gehaltene Informationen, die das Informationssicherheitsmanagement und/oder den IT-Betrieb betreffen, sofern der Beurteiler einen entsprechend berechtigtes Interesse glaubhaft machen kann. Dieser muss im letzten Fall entsprechend der „Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen“ (VSA – siehe [BMI2]) bzw. dem Handbuch für den Geheimschutz in der Wirtschaft (siehe [BMWI]) sicherheitsüberprüft und ermächtigt sein. Dabei ist die Stufe der Sicherheitsüberprüfung vom Vertraulichkeitsgrad der betreffenden Informationen abhängig.

Grundlagen für den Cyber-Sicherheits-Check sind neben diesem Leitfaden die beiden BSI-Empfehlungen zur Cyber-Sicherheit „Basismaßnahmen der Cyber-Sicherheit“ (siehe [ACS3]) und „Cyber-Sicherheits-Exposition“ (siehe [ACS2]). Insofern diese Werke zu einzelnen Teilen des Beurteilungsgegenstands keine Aussage treffen, sind andere einschlägige Vorschriften, Gesetze, Standards oder Vorgaben durch Hersteller oder Berufsverbände zu verwenden. Die Nutzung dieser Regelwerke ist im Beurteilungsbericht zu dokumentieren und zu begründen.

Die Vor-Ort-Beurteilung kann sowohl von einem Beurteiler allein, als auch in einem Team von mehreren Personen durchgeführt werden. Grundsätzlich sollte bereits bei der Initiierung eines Cyber-Sicherheits-Checks beachtet werden, dass der laufende Betrieb in der Institution durch die Beurteilung nicht wesentlich gestört wird.

Der Beurteiler greift niemals selbst aktiv in Systeme ein und erteilt auch keine Handlungsanweisungen zu Änderungen an IT-Systemen, Infrastrukturen, Dokumenten oder organisatorischen Abläufen. Er benötigt jeweils ausschließlich lesenden Zugriff.

3.4 Durchführung eines Cyber-Sicherheits-Checks

3.4.1 Beurteilungsgegenstand

Gegenstand eines Cyber-Sicherheits-Checks ist grundsätzlich die gesamte Institution einschließlich ihrer Anbindungen an das Internet, der Anbindungen über andere Organisationseinheiten an das Internet sowie aller Anbindungen an weitere Netze, wie z.B. Netze von Partnern, Dienstleistern und Kunden.

Nicht relevant sind alle Aspekte, die physischen Zugang zu IT-Systemen betreffen bzw. Aspekte, die sich mit der physischen Sicherheit (Brandschutz, Einbruchsschutz etc.) beschäftigen.

3.4.2 Vorgehensweise

Schritt 1 – „Auftragserteilung“:

Zur Durchführung eines Cyber-Sicherheits-Checks müssen weder die obligatorischen Dokumente zum Sicherheitsprozess existieren, noch muss ein definierter Umsetzungsstatus bestimmter Sicherheitsmaßnahmen erreicht sein. Daher ist es möglich, einen Cyber-Sicherheits-Check in jedem Umfeld und in jedem Stadium des Sicherheitsprozesses zu initiieren.

Um eine umfangreiche und wirksame Beurteilung sicherzustellen, sollte der Auftrag zur Durchführung eines Cyber-Sicherheits-Checks durch die Leitung / das Management der betreffenden Institution erfolgen.

Schritt 2 – „Bestimmung der Cyber-Sicherheits-Exposition“:

Zur Risikoersteinschätzung für die zu beurteilende Institution wird vor der Vor-Ort-Beurteilung die Cyber-Sicherheits-Exposition bestimmt. Darauf basierend kann der zu erwartende Zeitaufwand, die Beurteilungstiefe sowie die Wahl der Stichproben risikoorientiert bestimmt werden.

Schritt 3 – „Dokumentensichtung“:

Die Dokumentensichtung dient dazu, einen Überblick über die Aufgaben, die Organisation und die IT-Infrastrukturen der Institution zu gewinnen. Die Dokumentensichtung beinhaltet lediglich eine grobe Sichtung der zur Verfügung gestellten Dokumente. Hierbei werden (soweit vorliegend) insbesondere das IT-Rahmenkonzept, die Liste der kritischen Geschäftsprozesse, die Sicherheitsleitlinie und das Sicherheitskonzept inklusive Netzplan beurteilt.

Sind keine ausreichend informativen Dokumente vorhanden, wird die Sichtung durch Gespräche ergänzt, in denen sich der Beurteiler den erforderlichen Überblick verschaffen kann. Auf Basis der gewonnenen Erkenntnisse bestimmt der Beurteiler risikoorientiert die Stichproben und Schwerpunkte der Beurteilung.

Schritt 4 – „Vorbereitung der Vor-Ort-Beurteilung“

Zur Vorbereitung der Vor-Ort-Beurteilung sollte ein Ablaufplan unter Einbeziehung der Cyber-Sicherheits-Exposition erstellt werden. Dieser stellt dar, welche Inhalte wann beurteilt werden sollen und welche Ansprechpartner (Rollen/Funktionen) hierzu erforderlich sind. Der Ablaufplan ist der betreffenden Institution vorab zu übersenden.

Schritt 5 – „Vor-Ort-Beurteilung“:

Die Vor-Ort-Beurteilung selbst beginnt immer mit einem kurzen Eröffnungs- und endet mit einem Abschlussgespräch. Im Eröffnungsgespräch wird der Institution die Vorgehensweise und Zielrichtung des Cyber-Sicherheits-Checks erläutert. Außerdem werden organisatorische Punkte geklärt, wie z.B. Zutrittskontrolle, Besprechungsraum oder etwaige Änderungen zum Ablauf.

Im Rahmen der Vor-Ort-Beurteilung werden Interviews geführt, IT-Systeme in Augenschein genommen und evtl. weitere Dokumente gesichtet. Bei der Durchführung der Vor-Ort-Beurteilung sollten die für die jeweiligen Themen zu befragenden Ansprechpartner zur Verfügung stehen. Die zu beurteilenden Stichproben (z.B. Dokumente, IT-Systeme) und die festgestellten Sachverhalte sollten vom Beurteiler ausreichend detailliert dokumentiert werden, um diese Informationen später für die Erstellung des Berichtes angemessen verwenden zu können.

Im Abschlussgespräch, an dem auch die Leitungsebene der Institution teilnehmen sollte, wird eine erste allgemeine Einschätzung zum Niveau der Cyber-Sicherheit in der Institution gegeben. Darüber hinaus eröffnet der Beurteiler schwerwiegende Sicherheitsmängel, die die Cyber-Sicherheit der Institution unmittelbar stark gefährden und deshalb zeitnah behandelt werden sollten.

Schritt 6 - „Nachbereitung / Berichterstellung“:

Der Cyber-Sicherheits-Check wird mit einem Beurteilungsbericht abgeschlossen. Dieser eröffnet einen Überblick zur Cyber-Sicherheit in der Institution und beinhaltet neben der Darlegung der Cyber-Sicherheits-Exposition eine Liste der festgestellten Mängel. Zu jedem Maßnahmenziel (siehe [ACS4]) sollte das jeweilige Beurteilungsergebnis dokumentiert werden. Im Bericht werden allgemeine Empfehlungen zur Behandlung der festgestellten Mängel aufgezeigt. Hieraus kann die beurteilte Institution entnehmen, in welchen Bereichen vermehrt Aktivitäten erforderlich sind, um das Cyber-Sicherheits-Niveau zu erhöhen.

3.4.3 Beurteilungsmethoden

Unter „Beurteilungsmethoden“ werden alle für die Ermittlung eines Sachverhaltes verwendeten Handlungen verstanden. Während eines Cyber-Sicherheits-Checks können vom Beurteiler folgende Beurteilungsmethoden genutzt werden:

- Mündliche Befragung (Interview),
- Inaugenscheinnahme von IT-Systemen, Orten, Räumlichkeiten und Gegenständen,
- Beobachtung (Wahrnehmungen im Rahmen der Vor-Ort-Beurteilung),
- Aktenanalyse (hierzu gehören auch elektronische Daten oder statistische Auswertungen),
- Datenanalyse (z.B. Konfigurationsdateien, Logfiles, Auswertung von Datenbanken etc.) und
- Schriftliche Befragung (z.B. Fragebogen).

3.4.4 Verbindliche Maßnahmenziele

Durch die Etablierung verbindlicher Maßnahmenziele soll sowohl eine gleichbleibend hohe Qualität des Cyber-Sicherheits-Checks, als auch eine Vergleichbarkeit der Tätigkeit unterschiedlicher Beurteiler gewährleistet werden.

Die Beurteilungstiefe (Intensität) wird vom Beurteiler, je nach Höhe der Cyber-Sicherheits-Exposition, risikoorientiert angepasst.

Die verbindlichen Maßnahmenziele für einen Cyber-Sicherheits-Check basieren auf den „Basismaßnahmen der Cyber-Sicherheit“ (siehe [ACS3]). Als besonderen Mehrwert stellen BSI und ISACA darüber hinaus eine Zuordnung der zu beurteilenden Maßnahmenziele zu bekannten Standards der Informationssicherheit (IT-Grundschutz, ISO 27001, COBIT, PCI DSS) zur Verfügung. Eine detaillierte Darstellung der verbindlichen Maßnahmenziele findet sich auf den Webseiten der Allianz für Cyber-Sicherheit (siehe [ACS4]).

3.4.5 Bewertungsschema

Werden im Rahmen eines Cyber-Sicherheits-Checks Sicherheitsmängel festgestellt, so hat der Beurteiler spätestens bei der Berichtserstellung festzulegen, wie diese in ihrer Kritikalität zu bewerten sind.

Sicherheitsmängel sind wie folgt einzuordnen:

- **„Kein Sicherheitsmangel“**
  Zum Zeitpunkt der Beurteilung konnte kein Sicherheitsmangel festgestellt werden. Es gibt keine ergänzenden Hinweise.
- **„Sicherheitsempfehlung“**
  Eine Sicherheitsempfehlung kann vorliegen, wenn einige der Maßnahmenempfehlungen

umgesetzt sind, andere noch nicht oder nur teilweise. Auch eine voll umgesetzte IT-Sicherheitsmaßnahme kann um eine Sicherheitsempfehlung ergänzt werden. Durch die Umsetzung der im Sachverhalt beschriebenen Maßnahmenempfehlungen kann die Sicherheit erhöht werden. Verbesserungsvorschläge für die Umsetzung von Maßnahmen, ergänzende Maßnahmen, die sich in der Praxis bewährt haben oder Kommentare hinsichtlich der Angemessenheit von Maßnahmen können ebenfalls als Sicherheitsempfehlung aufgeführt werden.

- **„Sicherheitsmangel“**
  Bei einem „Sicherheitsmangel“ liegt eine Sicherheitslücke vor, die mittelfristig behoben werden sollte. Die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen kann beeinträchtigt sein.
- **„Schwerwiegender Sicherheitsmangel“**
  Ein „schwerwiegender Sicherheitsmangel“ ist eine Sicherheitslücke, die umgehend geschlossen werden sollte, da die Vertraulichkeit, die Integrität und/oder die Verfügbarkeit der Informationen stark gefährdet und erheblicher Schaden zu erwarten ist. Sicherheitsmängel und -empfehlungen sind im Abschlussbericht so zu dokumentieren, dass die Bewertung für einen sachkundigen Dritten nachvollziehbar ist.

3.4.6 Erstellung des Beurteilungsberichtes

Der Beurteilungsbericht eines Cyber-Sicherheits-Checks ist der Leitung / dem Management der Institution bzw. dem Auftraggeber schriftlich bekannt zu geben. Eine Entwurfsversion des Berichts sollte der geprüften Institution vorab übermittelt werden, um zu verifizieren, ob die festgestellten Sachverhalte (nur festgestellte Sachverhalte – ohne Bewertungen und Empfehlungen) sachlich richtig aufgenommen wurden.

Der Beurteilungsbericht besteht mindestens aus folgenden drei Teilen:

1. den Rahmendaten, inklusive detaillierter Beschreibung des Beurteilungsgegenstands
2. einer Zusammenfassung (Management Summary, einschließlich Cyber-Sicherheits-Exposition)
3. der Detailbeurteilung (ausführliche Darstellung der festgestellten Mängel, deren Bewertung und Empfehlungen zum Abstellen der Mängel)

Der Beurteilungsbericht ist als Mängelbericht ohne Würdigung positiver Aspekte zu erstellen.

3.5 Positionierung des Cyber-Sicherheits-Checks

Den Cyber-Sicherheits-Check charakterisieren primär drei Merkmale, mit denen sich dieser von den anderen Audit-/Prüfverfahren des BSI (z.B. ISO27001 Audit auf der Basis von IT-Grundschutz, IS-Querschnittsrevision, IS-Kurzrevision) abgrenzen lässt. Dies sind:

1. Grundlage(n)
2. Grundlage für die Durchführung eines Cyber-Sicherheits-Checks ist der Leitfaden Cyber-Sicherheits-Check i.V.m. den beiden Cyber-Sicherheits-Empfehlungen „Basismaßnahmen der Cyber-Sicherheit“ sowie „Cyber-Sicherheits-Exposition“.
3. Modellierung nach IT-Grundschutz
4. Eine Modellierung nach IT-Grundschutz ist für die Durchführung eines Cyber-Sicherheits-Checks nicht zwingend erforderlich.
5. Umsetzung von IT-Grundschutz

6. Auch die Umsetzung von IT-Grundschutz bzw. das Erreichen eines bestimmten Niveaus der Umsetzung von IT-Grundschutz ist ebenfalls nicht notwendig, um einen Cyber-Sicherheits-Check durchführen zu können.

Zur Durchführung eines Cyber-Sicherheits-Checks werden explizit keine obligatorischen Voraussetzungen an Dokumentenlage oder Umsetzungsstatus gestellt. Dies soll es auch kleinen und mittelständischen Unternehmen oder Behörden, die sich bislang weniger intensiv mit dem Thema Cyber-Sicherheit beschäftigt haben, ermöglichen, einen Einstieg zu finden und für die Thematik sensibilisieren.

3.6 Weiterbildung zum Cyber-Security-Practitioner (CSP)

Einen Cyber-Sicherheits-Check kann eine Institution sowohl durch qualifiziertes eigenes Personal als auch durch einen kompetenten Dienstleister durchführen lassen. In beiden Fällen ist jedoch sicherzustellen, dass die in diesem Leitfaden vorgegebene Herangehensweise genutzt wird. Um die Kenntnis der wesentlichen Prinzipien der Cyber-Sicherheit und der Durchführung von Cyber-Sicherheits-Checks nach außen hin zu dokumentieren, bieten die Allianz für Cyber-Sicherheit und ISACA interessierten Teilnehmern in einer eintägigen Fortbildung zum Thema Cyber-Sicherheit die Möglichkeit, nach erfolgreichem Ablegen einer Multiple-Choice-Prüfung das Zertifikat als „Cyber-Security-Practitioner“ zu erlangen. Das Zertifikat ist 3 Jahre lang gültig und dann durch entsprechende Fortbildungsveranstaltungen zu erneuern.

Die eintägige Veranstaltung wird durch das BSI und ISACA als CPE-fähige Fortbildung für Zertifikatsinhaber der beiden Organisationen anerkannt.

4 Fazit & Ausblick

Der Leitfaden Cyber-Sicherheits-Check beschreibt eine praxisnahe Vorgehensweise zur Beurteilung der Cyber-Sicherheit in Unternehmen und Behörden und beinhaltet mit den verbindlichen Maßnahmenzielen konkrete Vorgaben zur Beurteilung erfahrungsgemäß häufig problembehafteter Themen.

Mit dieser auch international beachtenswerten Initiative hoffen die Allianz für Cyber-Sicherheit im BSI und das ISACA Germany Chapter einen wertvollen Beitrag zur Erhöhung der Cyber-Sicherheit in Unternehmen und Behörden geleistet zu haben.

Der Leitfaden und die verbindlichen Maßnahmenziele sollen kontinuierlich weiterentwickelt und an aktuelle Gegebenheiten angepasst werden.

Anregungen, Kritik und Lob werden gerne unter info@cyber-allianz.de angenommen.

Literatur

[ACS] Allianz für Cyber-Sicherheit, www.allianz-fuer-cybersicherheit.de

[ACS1] Allianz für Cyber-Sicherheit, BSI-CS_013 „Cyber-Sicherheits-Exposition“, www.allianz-fuer-cybersicherheit.de

[ACS2] Allianz für Cyber-Sicherheit, BSI-CS_0006 „Basismaßnahmen der Cyber-Sicherheit“, www.allianz-fuer-cybersicherheit.de

[ACS3] Allianz für Cyber-Sicherheit, BSI-CS_072 „Basismaßnahmen der Cyber-Sicherheit“, www.allianz-fuer-cybersicherheit.de

[ACS4] Allianz für Cyber-Sicherheit, Verbindliche Maßnahmenziele für den Cyber-Sicherheits-Check, www.allianz-fuer-cybersicherheit.de

[BMI1] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, Feb- ruar 2011, www.bmi.bund.de

[BMI2] Bundesministerium des Innern, Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen, Juni 2006, www.verwaltungsvorschriften-im-internet.de

[BMWI] Bundesministerium für Wirtschaft und Energie, Handbuch für den Geheimschutz in der Wirtschaft, November 2004, www.bmwi.de

[BITKOM] BITKOM e.V. , Studie IT-Sicherheit in Unternehmen, www.bitkom.org

[ISACA] ISACA Germany Chapter e.V., Webauftritt, www.isaca.de

[OECD] OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing.