Bundesamt
für Sicherheit in der
Informationstechnik

ISACA®
Trust in, and value from, information systems
Germany Chapter

Leitfaden Cyber-Sicherheits-Check

Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden

Inhaltsverzeichnis

Allianz für Cyber-Sicherheit

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

Als Zusammenschluss wichtiger Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz zum Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Die Allianz für Cyber-Sicherheit unterstützt den Informations- und Erfahrungsaustausch zwischen den verschiedenen Akteuren aus Wirtschaft, Verwaltung und Wissenschaft und erweitert darauf aufbauend kontinuierlich eine umfangreiche Wissensbasis.

Wirtschaftsunternehmen sind aufgerufen, sich aktiv in die Allianz für Cyber-Sicherheit einzubringen und den Erfahrungsaustausch zu stärken. Indem sie dem BSI beispielsweise mitteilen, mit welchen neuartigen Bedrohungen oder IT-Sicherheitsvorfällen die Unternehmen konfrontiert sind, tragen sie zur Erstellung eines vollständigen Lagebilds bei und helfen, noch zielgerichteter gegen Cyber-Angriffe agieren zu können. Gleichzeitig profitieren auch die Unternehmen von gemeinsam gewonnenen Erkenntnissen und Erfahrungen.

Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.

Mit seinen derzeit rund 600 Mitarbeiterinnen und Mitarbeitern und 88 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Die Angebote der Behörde richten sich dabei an die öffentliche Verwaltung in Bund, Ländern und Kommunen ebenso wie an Wirtschaftsunternehmen und Bürger. Das BSI untersucht und bewertet bestehende IT-Sicherheitsrisiken und schätzt die Auswirkungen neuer Entwicklungen ab. Zunehmend beobachtet das BSI eine Vielzahl von gezielten sowie ungezielten Cyber-Angriffen. Aufbauend darauf zieht das BSI Schlussfolgerungen in Bezug auf die Verbesserung der IT-Sicherheit in Deutschland. So erarbeitet das BSI beispielsweise Mindeststandards und Handlungsempfehlungen zur IT- und Internet-Sicherheit für verschiedene Zielgruppen, damit Risiken in Zukunft erst gar nicht entstehen.

„Heute kann sich keine Branche und kein Unternehmen vor Cyber-Angriffen sicher wähnen. Das zeigen die zahlreichen Vorfälle der jüngeren Zeit."

Dr. Hartmut Isselhorst,
Abteilungspräsident Cyber-Sicherheit,
BSI

ISACA Germany Chapter e.V.

Das ISACA Germany Chapter e.V. ist der deutsche Zweig des weltweit führenden Berufsverbandes der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten. Der Verein wurde 1986 gegründet und ist mit über 2.300 Mitgliedern Teil des internationalen Verbandes ISACA, dem weltweit mehr als 100.000 Know-how-Träger in über 180 Ländern der Welt angehören. Zweck des Vereins ist es, durch Diskussion und Informationsaustausch zwischen den Mitgliedern und Interessenten das Verständnis der Probleme auf dem Gebiet der IT-Revision, IT-Sicherheit sowie IT-Governance zu fördern und diese Erfahrungen durch Publikationen und Seminare allen Mitgliedern und Interessenten zur Kenntnis zu bringen sowie die Kontakte zwischen den Mitgliedern und Interessenten durch gesellschaftliche Veranstaltungen zu unterstützen und zu ergänzen. Darüber hinaus soll der Verein zur Förderung des Berufsbildes der IT-Revisoren, IT-Sicherheitsmanager sowie der IT-Governance-Beauftragten beitragen.

„Der Herr seiner Daten zu sein, ist angesichts der aktuellen Entwicklungen wichtiger denn je. Nur wenn Institutionen ihr Wissen schützen können, behalten sie ihren Vorsprung."

Andreas Teuscher,
Vorstand des Ressort Facharbeit und Arbeitskreise,
ISACA Germany Chapter e.V.

Kooperation BSI / ISACA

Dieser Leitfaden wurde durch das ISACA Germany Chapter e.V. Ressort Facharbeit und Arbeitskreise (Fachgruppe Informationssicherheit) 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.

1 Einleitung

1 Einleitung

Die meisten Geschäftsprozesse hängen heute vom verlässlichen und fehlerfreien Funktionieren der Informations- und Kommunikationstechnik ab. Viele Ratingagenturen bewerten daher die Sicherheit der Informationstechnik schon als Teil der operationellen Risiken eines Unternehmens. Die tatsächlichen Bedrohungen, ebenso wie die Schadenshöhe erfolgreicher Cyber-Angriffe, sind nicht immer offensichtlich: So sind beispielsweise die Konsequenzen eines Know-how-Diebstahls möglicherweise erst sehr viel später erkennbar.

Umfragen zufolge waren bereits über 70 Prozent der größeren Unternehmen in Deutschland von Cyber-Angriffen betroffen. Dabei nehmen Anzahl, Komplexität und Professionalität der Angriffe zu. Die trotzdem in vielen Unternehmen immer noch verbreitete Einstellung „Bisher ist ja auch nichts passiert" kann daher schnell zu ernsthaften Problemen führen, wenn die bestehenden Sicherheitskonzepte nicht kontinuierlich und angemessen an die geänderte Bedrohungslage angepasst werden. Unabhängig davon nimmt die Anzahl der Bedrohungen stetig zu, womit auch die Wahrscheinlichkeit, dass ein Unternehmen oder eine Behörde von einem Cyber-Angriff betroffen ist, rasant ansteigt. Je nach Abhängigkeit von der IT kann die Unternehmenstätigkeit komplett zum Stillstand gebracht werden – mit allen Konsequenzen, die damit verbunden sind. Cyber-Sicherheit sollte daher Chefsache sein.

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 Grunde 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]).

Die Dauer eines Cyber-Sicherheits-Checks kann durch Anpassung der Beurteilungstiefe an die zu beurteilende Institution und die gegebenen Rahmenbedingungen von einem bis zu mehreren Tagen modifiziert werden. Ein Cyber-Sicherheits-Check kann sowohl durch qualifiziertes, eigenes Personal, als auch durch externe Dienstleister, die ihre Kompetenz zur Durchführung von Cyber-Sicherheits-Checks durch eine Personenzertifizierung zum „Cyber-Security-Practitioner“ nachgewiesen haben, durchgeführt werden. Als besonders interessanten 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 Mustervorlage für einen Abschlussbericht, der in kompakter Form sowohl die festgestellten Mängel, als auch Empfehlungen zum Abstellen dieser Mängel darstellt, vervollständigt die bereitgestellten Hilfsmittel zur Durchführung eines Cyber-Sicherheits-Checks.

Der vorliegende Leitfaden richtet sich an alle Interessenten, die sich direkt oder indirekt mit der Cyber-Sicherheit befassen. Aufgrund der Relevanz und Wichtigkeit dieses Themas sollten sich alle Ebenen, also Leitung / Management einer Institution, Information Security Manager / IT-Sicherheitsbeauftragte, Corporate Security Manager, IT-Administratoren und IT-Revisoren bis hin zum Endanwender mit Cyber-Sicherheit befassen. Dieses Dokument ist als Orientierungshilfe für Einsteiger und als Handlungsanleitung für Verantwortliche, die einen Cyber-Sicherheits-Check veranlassen oder durchführen möchten, gedacht.

Der vorliegende Leitfaden liefert konkrete Vorgaben für die Durchführung eines Cyber-Sicherheits-Checks, welche insbesondere in Kapitel 4 „Durchführung eines Cyber-Sicherheits-Checks“ zu finden sind. IT-Sicherheitsbeauftragten und sonsti-

gen Verantwortlichen für die Informationssicherheit soll dieser Leitfaden insbesondere dazu dienen, sich einen Überblick über das Thema zu verschaffen, die zu beurteilenden Sicherheitsaspekte zu betrachten und sich mit dem Ablauf eines Cyber-Sicherheits-Checks vertraut zu machen.

Dieser Leitfaden bildet die Grundlage für die Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden.

Revisoren und Beratern wird ein praxisnaher Handlungsleitfaden zur Verfügung gestellt, der konkrete Vorgaben und Hinweise für die Durchführung eines Cyber-Sicherheits-Checks und die Berichtserstellung enthält. Die Vereinheitlichung der Vorgehensweise gewährleistet eine gleichbleibend hohe Qualität. Darüber hinaus soll hierdurch die Transparenz für Unternehmen und Behörden beim Vergleich unterschiedlicher Angebote im Rahmen der Ausschreibung und Beauftragung der Dienstleistung „Cyber-Sicherheits-Check“ erhöht werden.

Das Bundesamt für Sicherheit in der Informationstechnik und das ISACA Germany Chapter e.V. bedanken sich bei den Autoren der ISACA-Fachgruppe Informationssicherheit: Matthias Becker, Olaf Bormann, Ingrid Dubois, Gerhard Funk, Oliver Knörle, Andrea Rupprich, Dr. Tim Sattler und Andreas Teuscher.

2 Einführung in die Cyber-Sicherheit

2 Einführung in die Cyber-Sicherheit

2.1 Was ist 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 Begriff „Cyber“ im Kontext der Informationssicherheit erfordert jedoch eine zusätzliche Erklärung, da er oft missverstanden oder verallgemeinert wird. Im Hinblick auf diesen Leitfaden umfasst Cyber-Sicherheit die Überprüfung getroffener Sicherheitsmaßnahmen mittels Cyber-Sicherheits-Checks,

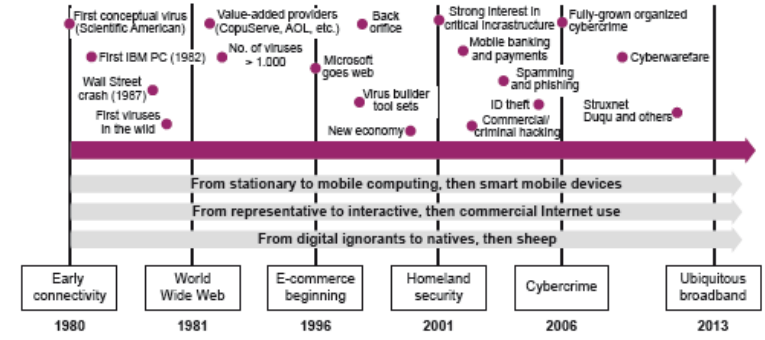


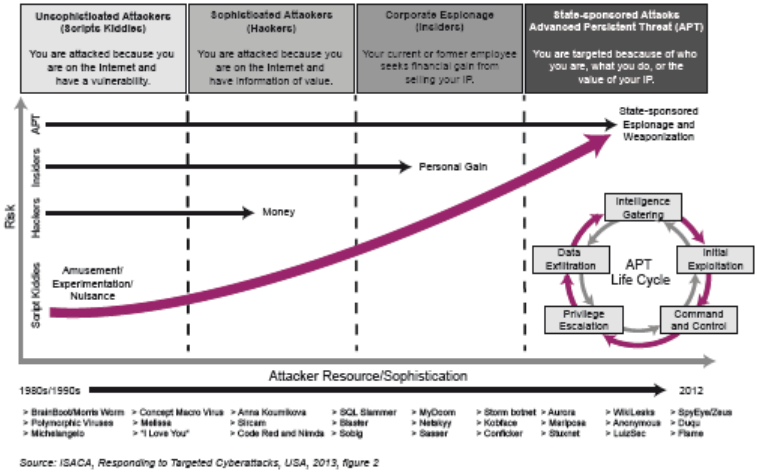
Abbildung 1: Entwicklung im Cyber-Raum (aus [ISACA2])

die Institutionen und Einzelpersonen davor bewahren soll, Opfer eines Cyber-Angriffs, von Cyber-Kriminalität oder Cyber-Kriegsführung zu werden. In der Praxis beschränkt sich Cyber-Sicherheit jedoch auf fortgeschrittene und zielgerichtete Angriffe, die nur schwer zu entdecken und abzuwehren sind (siehe Advanced Persistent Threats (APTs)). Cyber-Sicherheit ist somit ein Teil der generellen Kriminalitätsbekämpfung, wobei die Täter bei ihren Angriffen bewusst und gezielt Informationstechnologie als Waffe einsetzen.

Wie in Abbildung 1 dargestellt ist, hat Cyber-Sicherheit eine Geschichte, die bis in die frühen 1980er Jahre zurückreicht, als Kriminelle begannen, technische Angriffe in Form von Hacking, Cracking und Schadprogrammen (z. B. Viren, Würmer und Trojanische Pferde) für ihre Zwecke einzusetzen. Erst in den vergangenen Jahren aber haben sich Cyber-Kriminalität und weit verbreitete Cyber-Angriffe zu einem gesellschaftlichen und wirtschaftlichen Problem entwickelt.

2.2 Cyber-Angriffe und Advanced Persistent Threats (APTs)

Institutionen müssen sich täglich mit Bedrohungen, Risikoszenarien und Schwachstellen auseinandersetzen. Die höchste Gefährdung für Unternehmen und Behörden sowie deren Partner stellen aktuell zielgerichtete Cyber-Angriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer dar. Diese Art der Angriffe wird häufig unter dem Begriff APT (Advanced Persistent Threat) zusammengefasst (siehe [ISACA7]). APTs sind sowohl in ihrer Vorbereitung als auch in ihrer Durchführung meist sehr komplex und werden typischerweise in mehreren Phasen vollzogen. Das Ziel eines APT ist es, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten. Diese Art von Cyber-Angriffen hat häufig einen professionellen Hintergrund (z. B. Cyber-Kriminalität oder Wirtschaftsspionage), ist schwer zu detektieren und die Angreifer sind nur mit erheblichem Aufwand zu identifizieren. Die folgende Abbildung zeigt, wie sich die Bedrohungen über die Zeit entwickelt haben und welche Motivation dahinter stecken kann.



Source: ISACA, Responding to Targeted Cyberattacks, USA, 2013, figure 2

Abbildung 2: Entwicklung der Bedrohungslandschaft (aus [ISACA7])

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 durch regelmäßige Durchführung eines Cyber-Sicherheits-Checks minimiert werden. Sofern eine Institution bereits Opfer eines APT-Angriffs wurde bzw. der Verdacht auf einen APT-Angriff besteht, können konkrete Maßnahmen zur Reaktion dem BSI-Dokument „Erste-Hilfe bei einem APT-Angriff“ (siehe [ACS5]) entnommen werden.

2.3 Auswirkungen der Cyber-Kriminalität auf Institutionen und Gesellschaft

Die Bedrohungen durch Cyber-Kriminalität und Cyber-Kriegsführung habe heute zahlreiche Auswirkungen auf die Gesellschaft, Institutionen und Betroffene. Seit 2006 kann beobachtet werden, dass sich das organisierte Verbrechen und von Regierungen motivierte Kriegsführungsstrategien damit beschäftigen, wie mögliche Ziele von Cyber-Angriffen aussehen könnten. Die Resultate waren:

» Diebstahl von vertraulichen Informationen, Produktdaten und Entwicklungen bis hin zur systematischen Spionage

» Diebstahl von geistigem Eigentum, Manipulation von Handelsgeschäften, Unterschlagung von Werten

» Finanzbetrug, Missbrauch von Kreditkarten, Fälschung und Missbrauch von Identitäten

Interessant dabei ist, dass die Entwicklung der Cyber-Kriminalität in ihrer gegenwärtigen Form eine Geschwindigkeit und eine Größenordnung erreicht hat, die selbst von Kritikern nicht prognostiziert wurde.

Die Cyber-Kriminalität wuchs im Vergleich zur allgemeinen Kriminalität von ca. 1% in 2009 auf 23% in 2011 und hat damit binnen kürzester Zeit einige andere Formen der Kriminalität überholt. Die Cyber-Kriegsführung, über die anfänglich nur vereinzelt Informationen, z. B. zu den Hintergründen der Schadprogramme Stuxnet und Duqu, bekannt geworden sind, zeigt sich mittlerweile durch die Veröffentlichungen des NSA-Whistleblowers Edward Snowden in ihrem wahren Ausmaß.

In beiden Fällen sind die Auswirkungen auf Gesellschaft, Institutionen und Betroffene immens und eine „Nicht-Teilnahme am Cyber-Raum“ scheint keine realistische Option mehr zu sein. Vielmehr muss die Erkenntnis erwachsen, dass jede Institution, die sich im Cyber-Raum bewegt, auch unweigerlich solchen Angriffen ausgesetzt ist. Die Leitung einer Institution sollte dieses Bewusstsein in ihre Risikobetrachtung mit aufnehmen und angemessene Ressourcen bereitstellen, um angemessene Schutzvorkehrungen umzusetzen.

2.4 Cyber-Sicherheitsstrategie der Bundesregierung

Der Cyber-Raum umfasst alle durch das Internet weltweit über territoriale Grenzen hinweg erreichbaren Informationsinfrastrukturen. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Möglichkeiten. Staat, Kritische Infra-

strukturen, Wirtschaft und Bevölkerung in Deutschland sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.

Im Rahmen des Umsetzungsplans Kritische Infrastrukturen (UP KRITIS) kooperiert das BSI bereits seit 2007 intensiv mit Betreibern Kritischer Infrastrukturen. Die „Cyber-Sicherheitsstrategie für Deutschland", die im Februar 2011 von der Bundesregierung beschlossen wurde, ermöglicht es Staat, Wirtschaft und Privatanwendern, im Rahmen ihrer jeweiligen Verantwortungsbereiche und Handlungsmöglichkeiten, aktuellen und künftigen Bedrohungen aus dem Cyber-Raum begegnen zu können. Cyber-Sicherheit wird dabei durch die im Vordergrund stehenden zivilen Ansätze und Maßnahmen als Teil der gesamtstaatlichen Sicherheitsvorsorge verankert. Bei den Kritischen Informationsstrukturen steht die stärkere Verzahnung von Staat und Wirtschaft auf der Grundlage eines intensiven Informationsaustausches im Mittelpunkt.

3 Grundsätze des Cyber-Sicherheits-Checks

3 Grundsätze des Cyber-Sicherheits-Checks

Mit Hilfe eines Cyber-Sicherheits-Checks können Unternehmen und Behörden das aktuelle Niveau der Cybersicherheit in ihrer Institution bestimmen. Wie aus der Informationssicherheit bekannt, muss eine solche Beurteilung auf Basis eines umfassenden Rahmenwerks erfolgen, um fundierte Aussagen liefern zu können. Der vorliegende Leitfaden und die zugrunde liegenden Maßnahmenziele für die Beurteilung wurden so konzipiert, dass das Risiko, einem Cyber-Angriff zum Opfer zu fallen, durch regelmäßige Durchführung eines Cyber-Sicherheits-Checks minimiert werden kann. Dabei wurde die Vorgehensweise auf Cyber-Sicherheits-Belange fokussiert. Sie setzt auf drei Verteidigungslinien auf.

Abbildung 3 zeigt, dass zuerst ein Verständnis der Leitung / des Managements einer Institution für die Notwendigkeit von Maßnahmen zur Cyber-Sicherheit, den Schutzbedarf der Geschäftsprozesse sowie deren Abhängigkeiten und Bedrohungen

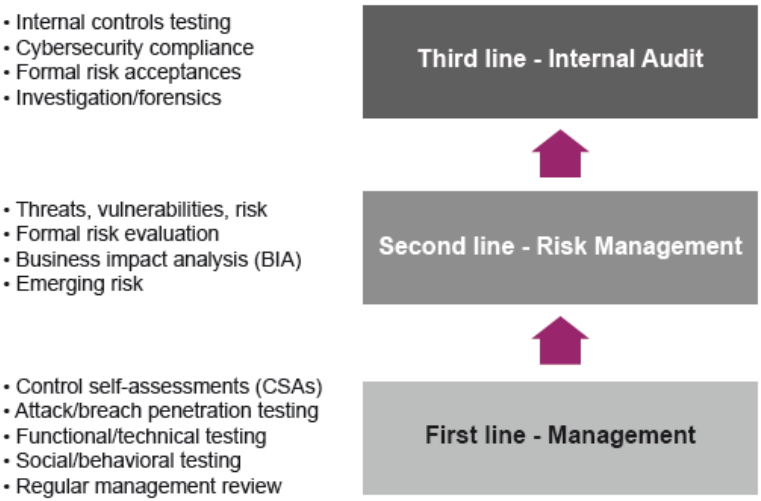


Abbildung 3: Drei Verteidigungslinien

vorhanden sein muss. Über das Risikomanagement, welches die zweite Linie darstellt, sollte es dann zu einer Analyse kommen, in wie weit sich Cyber-Sicherheitsrisiken auf die Institution und deren Prozesse auswirken. Dabei prüft das Risikomanagement der Institution als erste unabhängige Instanz die Entscheidungen der Leitung / des Managements und bewertet diese, allerdings ohne die Beschlüsse rückgängig zu machen. Die finale Entscheidung über die Umsetzung von Sicherheitsmaßnahmen verbleibt weiterhin bei der Leitung / dem Management.

Als dritte Verteidigungslinie kommt der Cyber-Sicherheits-Check zum Einsatz, durch den eine unabhängige und objektive Beurteilung des vorhandenen Sicherheitsniveaus erfolgt. Der Beurteiler unterstützt die Institution bei der Erreichung ihrer Ziele, indem er mit einem systematischen und zielgerichteten Ansatz die Cyber-Sicherheit in der Institution bewertet und durch seine Arbeit die Optimierung der Sicherheitsmaßnahmen fördert.

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) [ISACA8]

» Unabhängigkeit (siehe dazu ISACA IT-Prüfungsstandard 1002 – Organisatorische Unabhängigkeit und 1004 – Persönliche Unabhängigkeit) [ISACA8]

» Rechtschaffenheit und Vertraulichkeit (siehe dazu ISACA IT-Prüfungsstandard 1005 – Berufsübliche Sorgfalt) [ISACA8]

» Fachkompetenz (siehe dazu ISACA IT-Prüfungsstandard 1006 – Expertise) [ISACA8]

» Nachweise und Nachvollziehbarkeit (siehe dazu ISACA IT-Prüfungsstandard 1205 – Nachweise) [ISACA8]

» Objektivität und Sorgfalt (siehe dazu ISACA IT-Prüfungsstandards 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen und 1204 – Wesentlichkeit) [ISACA8]

» Sachliche Darstellung (siehe dazu ISACA IT-Prüfungsstandard 1401 – Berichterstattung) [ISACA8]

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 [BMI3]) 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.

4 Durchführung eines Cyber-Sicherheits-Checks

4 Durchführung eines Cyber-Sicherheits-Checks

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.

Sofern wesentliche logische IT-Systeme oder IT-Dienste von der Beurteilung ausgenommen werden, ist dies als Abgrenzung des Beurteilungsgegenstands im Beurteilungsbericht zu dokumentieren und zu begründen.

4.2 Vorgehensweise

Nachfolgend wird die Vorgehensweise zur Durchführung eines Cyber-Sicherheits-Checks schrittweise erläutert:

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.

Sofern die Bestimmung der Cyber-Sicherheits-Exposition für die betreffende Institution noch nicht auf Basis einer Management-Entscheidung durchgeführt wurde, sollte dies in geeigneter Weise durch den Beurteiler in Kooperation mit der Institution erfolgen. Entsprechende Anhaltspunkte liefern z. B. die in (siehe [ACS2]) vorgestellten Verfahrensweisen, vom Beurteiler geführte Kurzinterviews oder vorhandene Erfahrungswerte. Wurde die Cyber-Sicherheits-Exposition bereits durch die Institution bestimmt, kann der Beurteiler diese ohne weitere eigene Aktivitäten übernehmen, wenn ihm diese nachvollziehbar und angemessen erscheint. Die Ergebnisse der Cyber-Sicherheits-Exposition sind in jedem Fall im Bericht in geeigneter Weise zu dokumentieren.

Detaillierte Informationen zur Bestimmung der Cyber-Sicherheits-Exposition finden sich in der BSI-Empfehlung zur Cyber-Sicherheit BSI-CS_013 „Cyber-Sicherheits-Exposition“ (siehe [ACS2]).

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 Dokumentensichtung 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 Eröffnungsgespräch 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. Der Bericht 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.

Nähere Informationen zur Erstellung des Berichtes finden sich in Kapitel 4.6 „Erstellung des Beurteilungsberichtes“.

4.2.1 Qualität der Durchführung / Personenzertifikat

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 ein 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.

4.3 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).

Welche dieser Methoden angewendet werden, hängt vom konkreten Sachverhalt ab und ist durch den Beurteiler festzulegen. Dieser hat weiterhin zu beachten, dass in jedem Fall der Grundsatz der Verhältnismäßigkeit eingehalten wird. Für die Ermittlung eines Sachverhaltes können auch mehrere Beurteilungsmethoden kombiniert zur Anwendung kommen.

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 verbindlichen Maßnahmenziele für einen Cyber-Sicherheits-Check basieren auf den „Basismaßnahmen der Cyber-Sicherheit“ (siehe [ACS3]). Eine detaillierte Darstellung der

verbindlichen Maßnahmenziele findet sich auf den Webseiten der Allianz für Cyber-Sicherheit (siehe [ACS4]).

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

4.5 Bewertungsschema

Werden im Rahmen eines Cyber-Sicherheits-Checks Sicherheitsmängel festgestellt, so hat der Beurteiler spätestens bei der Berichtserstellung festzulegen, wie die betreffenden Mängel 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“
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.

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:

» den Rahmendaten, inklusive detaillierter Beschreibung des Beurteilungsgegenstands

» einer Zusammenfassung (Management Summary, einschließlich Cyber-Sicherheits-Exposition)

» 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.

Teil I - Rahmendaten

Dieser Teil enthält die organisatorischen Informationen:

» Beurteilungsgegenstand

» Abgrenzung des Beurteilungsgegenstands

» Beurteiler

» Ansprechpartner der beurteilten Institution

» Beurteilungsgrundlagen

» zeitlicher Ablauf

» Verteiler für den Beurteilungsbericht

» Rahmendaten des Beurteilungsdokuments bzw. der Dokumentenlenkung

- Dateiname
- Druckdatum
- Dokumentenstatus

Teil II - Management Summary

Dieser Teil enthält eine Zusammenfassung für das Management. In knapper, verständlicher Form sollten die wesentlichen Mängel und daraus hervorgehende Empfehlungen zusammengefasst werden.

» Summary

» Cyber-Sicherheits-Exposition

» Übersicht der Beurteilungsergebnisse
(für alle Maßnahmenziele aus (siehe [ACS4]))

Teil III - Detailbeurteilung je Maßnahmenziel

Dieser Teil des Berichtes beinhaltet die ausführliche Darstellung der beurteilten Themenfelder, die festgestellten Mängel, deren Bewertung sowie Empfehlungen zum Abstellen der bemängelten Sachverhalte. Bei der Bewertung der festgestellten Mängel ist das in Kapitel 4.5 dargestellte Schema zu verwenden.

» Maßnahmenziel (siehe [ACS4])

» Ergebnis einschließlich Bewertung

» Stichprobe(n)

» Beschreibung festgestellter Mängel inkl. Maßnahmenempfehlung(en)

Formale Aspekte zum Abschlussbericht:

Bei der Erstellung des Beurteilungsberichtes sind folgende formale Aspekte zu berücksichtigen:

» Die Seitenkennzeichnung muss so gestaltet sein, dass jede Seite eindeutig identifiziert werden kann (z. B. mit Seitennummer sowie Versionsnummer, Bezeichnung und Datum des Berichts).

» Verwendete Fachbegriffe oder Abkürzungen, die nicht allgemein gebräuchlich sind, müssen in einem Glossar bzw. Abkürzungsverzeichnis zusammengefasst werden.

» Der Bericht muss die geprüften Organisationseinheiten und die Empfänger des Berichts eindeutig bezeichnen sowie etwaige Verwendungsbeschränkungen vermerken.

» Der Bericht ist durch den Beurteiler zu unterschreiben.

» Form und Inhalt eines Berichts können je nach Art der in Auftrag gegebenen Beurteilungsarbeiten unterschiedlich sein, jedoch sind für den Cyber-Sicherheits-Check die Mindestan-

forderungen an den Beurteilungsbericht (siehe dieses Kapitel) sowie der ISACA IT-Prüfungsstandard 1401 (siehe [ISACA6]) einzuhalten.

Ein Muster-Bericht für einen Cyber-Sicherheits-Check findet sich auf den Webseiten der Allianz für Cyber-Sicherheit (siehe [ACS6]).

5 Glossar und Begriffsdefinition

5 Glossar und Begriffsdefinition

Die folgenden Begrifflichkeiten werden in diesem Dokument verwendet:

APT (Advanced Persistent Threat) bezeichnet einen sehr komplexen, zielgerichteten, aufwendig vorbereiteten und durchgeführten Cyber-Angriff (siehe auch Kapitel 2.2).

BSI (Bundesamt für Sicherheit in der Informationstechnik) ist der zentrale IT-Sicherheitsdienstleister der Bundesverwaltung.

Beurteiler ist eine Person, die einen Cyber-Sicherheits-Check auf Basis dieses Leitfadens durchführt.

CPE (Continuing Professional Education) ist ein Maß für die Erbringung von kontinuierlicher beruflicher Weiterbildung.

Cyber-Kriminalität sind kriminelle Aktivitäten, die den Cyber-Raum als Quelle, Ziel und/oder Werkzeug nutzen.

Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen.

Cyber-Sicherheit verfolgt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gegen Bedrohungen aus dem Cyber-Raum.

Institution wird als Oberbegriff für Behörden, Unternehmen und sonstige öffentliche oder private Organisationen verwendet.

ISACA (Information Systems Audit and Control Association) ist der Berufsverband der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten.

KRITIS (Kritische Infrastrukturen) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Leitung / Management wird als Begriff für Vorstand, Geschäftsführer, Behördenleitung verwendet.

Maßnahmenziele sind für die Beurteilung relevante Aspekte und Fragestellungen der Cyber-Sicherheit. Hierzu gehören Themen des Sicherheitsmanagements genauso wie technische Aspekte.

Whistleblower (auch ‚Enthüller', ‚Skandalaufdecker' oder ‚Hinweisgeber') ist eine Person, die für die Allgemeinheit wichtige Informationen aus einem geheimen oder geschützten Zusammenhang an die Öffentlichkeit bringt.

Alle Personalbegriffe in diesem Dokument beziehen sich in gleicher Weise auf Frauen und Männer. Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

6 Literaturverzeichnis

6 Literaturverzeichnis

[ACS1] Allianz für Cyber-Sicherheit, Webauftritt, www.allianz-fuer-cybersicherheit.de

[ACS2] Allianz für Cyber-Sicherheit, BSI-CS_013 „Cyber-Sicherheits-Exposition“, www.allianz-fuer-cybersicherheit.de

[ACS3] Allianz für Cyber-Sicherheit, BSI-CS_006 „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

[ACS5] Allianz für Cyber-Sicherheit, BSI-CS_072 „Erste-Hilfe bei einem APT-Angriff“, www.allianz-fuer-cybersicherheit.de

[ACS6] Allianz für Cyber-Sicherheit, Muster-Bericht für den Cyber-Sicherheits-Check, www.allianz-fuer-cybersicherheit.de

[BMI1] Bundesministerium des Innern, Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland, Umsetzungsplan KRITIS (UP-KRITIS), September 2007, www.bmi.bund.de

[BMI2] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, Februar 2011, www.bmi.bund.de

[BMI3] 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

[ISACA1] ISACA Germany Chapter e.V., Webauftritt, www.isaca.de

[ISACA2] ISACA, Transforming Cybersecurity Using COBIT® 5, 2013, www.isaca.org/cybersecurity-cobit

[ISACA3] ISACA, Berufs-Ehrenkodex, 2013, www.isaca.org

[ISACA4] ISACA, COBIT® 5 for Information Security, 2012, http://www.isaca.org/cobit5security

[ISACA5] ISACA, Responding to Targeted Cyberattacks, 2013, www.isaca.org/cyberattacks

[ISACA6] ISACA, IT-Prüfungsstandards, 2013, www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Audit-and-Assurance-German.aspx

[ISACA7] ISACA, Advanced Persistent Threats: How to Manage the Risk to Your Business, 2013, www.isaca.org/apt-book

[ISACA8] ISACA, Knowledge Center, www.isaca.org/Knowledge-Center

7 Maßnahmenziele

Erläuterung

Die nachfolgend aufgeführten Maßnahmenziele A bis M sind bei der Durchführung eines Cyber-Sicherheits-Checks verbindlich zu beurteilen. Die Reihenfolge der Maßnahmenziele ist dabei nicht als Priorisierung oder zwingende Abfolge bei der Beurteilung anzusehen, sondern dient lediglich der Strukturierung.

Zur Beurteilung eines Maßnahmenziels sind mindestens die zu dem jeweiligen Maßnahmenziel zugehörigen Basismaßnahmen heranzuziehen.

Die Stichproben für die Vor-Ort-Beurteilung sind nach einem risikoorientierten Ansatz zu prüfen.

Detaillierte Hinweise zur Durchführung eines Cyber-Sicherheits-Checks finden sich im Kapitel 4 des Leitfadens „Cyber-Sicherheits-Check“ (www.allianz-fuer-cybersicherheit.de).

	Maßnahmen	Basismaßnahmen	Referenzen
A	**Absicherung von Netzübergängen** Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet. Auf Grundlage der Netzwerkarchitektur müssen Abwehrmaßnahmen für alle internen und externen Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein Change Management) geplant und umgesetzt werden.	» Alle Netzübergänge sind identifiziert und dokumentiert. » Das Netz ist in Segmente aufgeteilt und die Anzahl der Netzübergänge wird minimal gehalten. » Alle Netzübergänge sind durch geeignete Sicherheitsgateways abgesichert und werden regelmäßig überprüft. » Auf Client- und Serversystemen findet eine technische Schnittstellenkontrolle statt, die eine zulässige Nutzung kontrolliert und eine unzulässige Nutzung verhindert. » Zugänge mobiler IT-Geräte sind angemessen abgesichert und auf das erforderliche Mindestmaß beschränkt. » Zugänge für Remote-Administration und -Überwachung sind angemessen abgesichert. » Es werden nur zeitgemäße Verschlüsselungs- und Authentisierungsverfahren eingesetzt.	**BSI IT-GSK 13. Erg.-Lieferung:** B 3.301, B 3.302, B 4.1, B 5.14, M 2.204 **COBIT 5:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2005:** A.10.6, A.10.7.1, A.11.4, A.11.6.2, A11.7, A.12.5.4 **ISO/IEC 27001:2013:** A.6.2, A.8.3.1, A.9.1.2, A.13.1 **PCI DSS 3.0:** 1.1, 1.1.2, 1.1.4, 1.1.6, 1.2, 1.2.3, 1.3, 1.3.1-1.3.8, 1.4, 2.2.3, 2.2.4, 4.1, 4.1.1, 8.3, 11.4, 12.3.8, 12.3.9

Maßnahmen		Basismaßnahmen	Referenzen
B	**Abwehr von Schadprogrammen** Im Sinne einer gestaffelten Verteidigung gegen Angriffe durch Schadprogramme (Viren, Würmer und Trojanische Pferde) muss die Abwehr über eine große Zahl von IT-Systemen einschließlich der Sicherheitsgateways verteilt werden. Der eigentliche Client als Arbeitsplatzsystem ist dabei die letzte Verteidigungslinie.	» Schutzsoftware gegen Schadprogramme kommt durchgängig zum Einsatz und wird fortlaufend aktuell gehalten. » Verteilt über die verschiedenen IT-Systeme kommen mehrere Lösungen unterschiedlicher Anbieter zum Einsatz (gestaffelte Verteidigung). » IT-Systeme ohne angemessenen Schutz vor Schadprogrammen sind in speziellen Netzsegmenten isoliert.	**BSI IT-GSK 13. Erg.-Lieferung:** B 1.6 **COBIT 5:** DSS05.01 **ISO/IEC 27001:2005:** A.10.4 **ISO/IEC 27001:2013:** A.12.2.1 **PCI DSS 3.0:** 5.1, 5.1.1, 5.1.2, 5.2, 5.3, 5.4
C	**Inventarisierung der IT-Systeme** Zur Planung und anschließenden Umsetzung von Abwehrmaßnahmen auf den eingesetzten IT-Systemen ist zunächst eine vollständige Inventarisierung der eingesetzten IT-Systeme und Software notwendig. Mithilfe dieses Inventarverzeichnisses ist insbesondere zu klären, welche verschiedenen Systemtypen in der Organisation im Einsatz sind.	» Der Bestand an Hard- und Software ist vollständig inventarisiert und wird fortlaufend aktualisiert. » Versionen und Patchstände von Betriebssystemen und Anwendungen werden regelmäßig aufgenommen. » Es existieren automatisierte Verfahren zur Erkennung nicht-autorisierter IT-Systeme und Anwendungen.	**BSI IT-GSK 13. Erg.-Lieferung:** M 2.10 **COBIT 5:** APO01.06, BAI03.04, BAI09.01, BAI09.05 **ISO/IEC 27001:2005:** A7.1.1, A.7.1.2 **ISO/IEC 27001:2013:** A.8.1.1, A.8.1.2 **PCI DSS 3.0:** 2.4, 9.7, 9.7.1, 11.1, 11.1.1, 12.3.3, 12.3.4

	Maßnahmen	Basismaßnahmen	Referenzen
D	**Vermeidung von offenen Sicherheitslücken** Um das Risiko erfolgreicher Cyber-Angriffe zu minimieren, müssen offene Sicherheitslücken konsequent vermieden werden. Vorhandene Sicherheitsmechanismen von Betriebssystemen sollten daher genutzt werden. Darüber hinaus sollten Sicherheitsaktualisierungen genutzter Software zeitnah getestet und anschließend installiert werden. Ein wirksamer Change-Managementprozess sollte etabliert werden.	» Ein effizienter Prozess zum Schwachstellen- und Patchmanagement ist etabliert. » Im Rahmen der Softwareplanung wird die Nutzung stärkerer Abwehrmechanismen in aktuellerer Software gefördert. » Bekannte Sicherheitslücken werden kurzfristig durch Workarounds und bereitgestellte Sicherheitsaktualisierungen geschlossen. » Betriebssysteme, Serverdienste und Anwendungen werden vor Inbetriebnahme gehärtet. » Ein Prozess zur sicheren Softwareentwicklung ist etabliert. » Bei der Beschaffung neuer Hard- und Software werden Sicherheitsanforderungen berücksichtigt.	**BSI IT-GSK 13. Erg.-Lieferung:** B 1.14, M 2.337 **COBIT 5:** APO12.01, BAI02.01, BAI10.02, BAI10.03, BAI10.05, DSS05.03 **ISO/IEC 27001:2005:** A.10.1.2, A.11.5.4, A.12.1.1, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3, A.12.6 **ISO/IEC 27001:2013:** A.9.4.4, A.12.1.2, A.12.5, A.12.6, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4 **PCI DSS 3.0:** 6.1, 6.2, 6.3, 6.3.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.4, 6.4.5, 6.5, 6.5.1–6.5.10

Maßnahmen		Basismaßnahmen	Referenzen
E	**Sichere Interaktion mit dem Internet** Alle Vorgänge, bei denen Daten und Dienste aus dem Internet abgefragt und verarbeitet werden, sind mit geeigneten Maßnahmen abzusichern. Die jeweilige Stärke der eingesetzten Schutzmechanismen muss dem Schutzbedarf der auf dem jeweiligen IT-System verarbeiteten Daten sowie den einem Angreifer zur Verfügung stehenden möglichen Weiterleitungsmechanismen gerecht werden.	» Der Browser inklusive aller Erweiterungen (Flash, Java, ActiveX usw.) verfügt über starke Sicherheitseigenschaften und ist bei einer hohen Cyber-Sicherheits-Exposition besonders abgeschottet (z.B. Sandbox). » Eingehender E-Mail-Verkehr wird zentral auf Bedrohungen, wie Schadprogramme und Phishing-Angriffe, untersucht. » Für die Darstellung von Dokumenten aus externen Quellen werden sichere Darstellungsoptionen verwendet. » Unerwünschte aktive Inhalte werden zentral gefiltert. » Apps und andere Internetanwendungen sind durch geeignete Schutzmechanismen abgesichert. » Es existieren verbindliche Vorgaben zur sicheren Nutzung von Cloud-Services und anderen Diensten im Internet.	**BSI IT-GSK 13. Erg.-Lieferung:** B 5.3, B 5.4, B 5.12, B 5.18, B 5.19, B 5.21, M 2.162, M 2.164, M 2.166, M 5.67, M 2.46, M 3.78, M 5.158 **COBIT 5:** BAI10.02, BAI10.03, BAI10.05, DSS05.01 **ISO/IEC 27001:2005:** A.6.2.3, A.10.4.2, A.10.8.4 **ISO/IEC 27001:2013:** A.13.2.3, A.15.1.2 **PCI DSS 3.0:** 1.4, 6.6, 12.3

	Maßnahmen	Basismaßnahmen	Referenzen
F	**Logdatenerfassung und –auswertung** Oftmals bleiben Sicherheitsvorfälle unerkannt, weil kurzfristig kein sichtbarer oder offensichtlicher Schaden eintritt. Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern aber u.U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden. Daher ist es notwendig, ebenfalls Verfahren zur Aufdeckung von nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen zu entwickeln.	» Relevante Logdaten werden gemäß einschlägiger gesetzlicher, regulatorischer und organisatorischer Anforderungen vollständig erfasst und regelmäßig ausgewertet. » Die Nutzung privilegierter Konten und administrativer Zugriffe wird fortlaufend überwacht. » Logdaten sind angemessen vor Manipulation und Zerstörung geschützt.	**BSI IT-GSK 13. Erg.-Lieferung:** B 5.22, M 2.64 **COBIT 5:** APO11.04, DSS05.07 **ISO/IEC 27001:2005:** A.10.10 **ISO/IEC 27001:2013:** A.12.4 **PCI DSS 3.0:** 10.1, 10.2, 10.2.2-10.2.7, 10.3, 10.3.1-10.3.6, 10.5, 10.5.1-10.5.5, 10.6, 10.6.1-10.6.3, 11.4
G	**Sicherstellung eines aktuellen Informationsstands** Die Fähigkeit zur Planung wirksamer Cyber-Sicherheits-Maßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Daher muss die Versorgung mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit sichergestellt werden.	» Aktuelle Informationen zur Cyber-Sicherheit werden fortlaufend aus verlässlichen Quellen bezogen und ausgewertet. » Cyber-Sicherheits-Maßnahmen werden regelmäßig auf der Basis vorhandener Informationen hinsichtlich ihrer Effektivität überprüft und angepasst.	**BSI IT-GSK 13. Erg.-Lieferung:** B 1.13, M 3.5,M 3.11, M 3.38, M 3.43, M 3.59, M 3.62, M 3.71, M 3.73 **COBIT 5:** APO12.01 **ISO/IEC 27001:2005:** A.6.1.7, A.13.1.2 **ISO/IEC 27001:2013:** A.6.1.4, A.16.1.3 **PCI DSS 3.0:** 6.1

	Maßnahmen	Basismaßnahmen	Referenzen
H	**Bewältigung von Sicherheitsvorfällen** Geeignete Prozesse und Verfahren zur Bewältigung von Sicherheitsvorfällen sind zu etablieren und zu üben, um eine schnelle und angemessene Bewältigung von Sicherheitsvorfällen und damit die Aufrechterhaltung des Geschäftsbetriebs sicherzustellen.	» Es existieren etablierte Prozesse und Verfahren zur schnellen und angemessenen Bewältigung von Sicherheitsvorfällen. » Die Bewältigung von Sicherheitsvorfällen wird regelmäßig geübt. » Abgeschlossene Sicherheitsvorfälle werden hinsichtlich der Ursachen und möglicher Konsequenzen ausgewertet. » Sicherheitsvorfälle werden zur Strafverfolgung und Lagebilderstellung an die zuständigen Behörden gemeldet.	**BSI IT-GSK 13. Erg.-Lieferung:** B 1.8 **COBIT 5:** DSS02.02, DSS02.02, DSS04.03, DSS05.01 **ISO/IEC 27001:2005:** A.13.1, A.13.2 **ISO/IEC 27001:2013:** A.16.1 **PCI DSS 3.0:** 12.10, 12.10.1-12.10.6
I	**Sichere Authentisierung** Zur sicheren Authentisierung von Benutzern sollten komplexe Passwörter und/oder Multifaktor-Authentisierungsverfahren genutzt werden. Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sollten voneinander getrennt werden.	» Der Zugang zu kritischen Ressourcen wird durch den Einsatz von Multifaktor-Authentisierungsverfahren abgesichert. » Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sind voneinander getrennt, z. B. Konten von Administratoren und anderen Nutzern. » Es werden nur sichere Authentisierungsprotokolle eingesetzt. » Authentisierungsdaten werden angemessen geschützt.	**BSI IT-GSK 13. Erg.-Lieferung:** B 5.15, M 2.6, M 2.7, M 2.8, M 4.133, M 4.176, M 4.250, M 4.392, M 5.59, M 5.160 **COBIT 5:** DSS05.04, DSS06.03 **ISO/IEC 27001:2005:** A.11.1.1, A.11.5.1, A.11.5.2 **ISO/IEC 27001:2013:** A.9.1.1, A.9.4.2 **PCI DSS 3.0:** 8.2, 8.2.1-8.2.6, 8.3, 8.4, 8.5, 8.5.1, 8.6

	Maßnahmen	Basismaßnahmen	Referenzen
J	**Gewährleistung der Verfügbarkeit notwendiger Ressourcen** Zur wirksamen Abwehr von Bedrohungen der Cyber-Sicherheit sollten ausreichend eigene finanzielle und personelle Ressourcen bereitgestellt und bei Bedarf auf qualifizierte externe Dienstleister zurückgegriffen werden.	» Finanzielle und personelle Ressourcen zur Abwehr von Bedrohungen der Cyber-Sicherheit stehen ausreichend zur Verfügung. » Bei Bedarf werden qualifizierte und zuverlässige externe Dienstleister eingebunden.	**BSI IT-GSK 13. Erg.-Lieferung:** M 2.1, M 2.2, M 2.193, M 2.226, M 2.337, M 2.339, M 3.3, M 3.51, M 4.392, M 5.59, M 5.160 **COBIT 5:** APO07.01, APO10.02 **ISO/IEC 27001:2005:** A.6.1.3 **ISO/IEC 27001:2013:** A.6.1.1 **PCI-DSS:** 12.4
K	**Durchführung nutzerorientierter Maßnahmen** Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.	» Anwender und IT-Personal werden zielgruppenorientiert regelmäßig für die Gefahren eines Cyber-Angriffs sensibilisiert und hinsichtlich des korrekten Verhaltens geschult. » IT-Personal und Management sind mit ihren Rollen und Verantwortlichkeiten vertraut. » Es ist eine klare Rollentrennung vorhanden. Eine Konzentration zu vieler Zuständigkeiten in einer Rolle wird vermieden.	**BSI IT-GSK 13. Erg.-Lieferung:** B 1.13, M 2.1, M 2.225, M 3.51 **COBIT 5:** APO07.02, APO07.03, DSS05.04, DSS06.03 **ISO/IEC 27001:2005:** A.8.2.2, A.10.1.3, A.15.1.5 **ISO/IEC 27001:2013:** A.6.1.2, A.7.2.2 **PCI DSS 3.0:** 6.4.2, 7.1, 7.1.1-7.1.4, 12.4.1, 12.6, 12.6.1, 12.6.2

	Maßnahmen	Basismaßnahmen	Referenzen
L	**Sichere Nutzung Sozialer Netzwerke** Die Sensibilisierung von Mitarbeitern muss insbesondere das Verhalten in Sozialen Netzwerken in Form verbindlicher Vorgaben (Social Media Guidelines) und Aufklärungsmaßnahmen umfassen.	» Es existieren verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile des Beschäftigten in Sozialen Netzwerken. » Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Verhaltens in Sozialen Netzwerken sensibilisiert. » Direkte Schnittstellen zwischen Sozialen Netzwerken und der organisationseigenen Infrastruktur, sofern vorhanden, sind angemessen abgesichert.	**BSI IT-GSK 13. Erg.-Lieferung:** M 3.5, M 5.157 **COBIT 5:** APO07.03 **ISO/IEC 27001:2005:** A.7.1.3, A.8.2.2,A.10.8.1 **ISO/IEC 27001:2013:** A.7.2.2, A.8.1.3, A.13.2.1, A.13.2.3 **PCI DSS 3.0:** n.a.
M	**Durchführung von Penetrationstests** Es sollten regelmäßige Penetrationstests von qualifizierten und erfahrenen Personen, die nicht an der Planung oder Implementierung der zu beurteilenden IT-Systeme beteiligt waren, durchgeführt werden.	» Es werden regelmäßig Penetrationstests von qualifizierten Personen durchgeführt. » Umfang und Intensität der Penetrationstests sind der Cyber-Sicherheits-Exposition angemessen. » Die Ergebnisse von Penetrationstests werden konsequent zur Reduzierung von Risiken genutzt.	**BSI IT-GSK 13. Erg.-Lieferung:** M 5.150 **COBIT 5:** APO12.01 **ISO/IEC 27001:2005:** A.6.1.8, A.15.2.2 **ISO/IEC 27001:2013:** A.14.2.8, A.18.2.1, A.18.2.3 **PCI DSS 3.0:** 11.3, 11.3.1-11.3.3

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger
www.allianz-fuer-cybersicherheit.de

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: info@cyber-allianz.de
Internet: www.bsi.bund.de
Telefon: +49 (0) 22899 9582 - 0
Telefax: +49 (0) 22899 9582 - 5400

Stand
Februar 2014

Druck
WM Druck + Verlag
53359 Rheinbach

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

www.bsi.bund.de