Beispiel Prüfung
Advanced Level Syllabus

Sicherheitstester
(Security Tester)

Fassung 2016
Deutsche Übersetzung 2019, V1.0

International Software Testing Qualifications Board

Deutschsprachige Ausgabe
Herausgegeben durch German Testing Board e.V.

Version	Datum	Bemerkung
1.0 Beta	22. Sept. 2015	Beta Version der Beispielprüfung
1.0-GA Kandidat	04. März 2016	Anpassungen nach Besprechung mit Exam Working Group – Frage 18 und 29 in K3 Level angehoben, Tippfehler in Frage 35 verbessert, Punktevergabe für Frage 25-32 angepasst.
1.0 - GA	15. März 2016	GA Version mit kleinen Veränderungen. Lernziele entfernt.
Version 2019	28. Feb. 2019	Übersetzung ins Deutsche

AS-1.1.1 (K2) Die Bedeutung der Risikobewertung als Informationsquelle für die Planung von Sicherheitstests und deren Ausrichtung an geschäftlichen Erfordernissen verstehen

AS-1.3.1 (K2) Den Zweck eines Sicherheitsaudits kennen[1]

Frage #1 (1 Punkt)

Welche der folgenden Antworten spiegelt die Absicht eines Sicherheitsaudits wider?

a) Benutzer daran hindern, einfache Passwörter zu nutzen

b) Inadäquate Updates vom Verkäufer erkennen

c) Unautorisierten Angreifern den Zugriff auf das System zu verbieten

d) Benutzern vorschreiben, ihr Passwort nach einer vorgeschriebenen Anzahl von Tagen zu ändern

B ist richtig, da eines der Ziele eines Sicherheitsaudits das Aktualisieren von Updates auf dem System ist. Die anderen Möglichkeiten sind gute Methoden, aber nicht der Zweck eines Sicherheitsaudits.

[1] Das Lernziel für die jeweilige Frage ist im gesamten Dokument farblich markiert. Für einige Fragen gibt es mehrere markierte Lernziele, auf die sich die Frage bezieht.

AS-1.1.2 (K4) Die wichtigen, zu schützenden, Assets identifizieren und den Wert der einzelnen Assets sowie der benötigten Daten für die Ermittlung ihrer Sicherheitsstufe ermitteln können

AS-1.1.3 (K4) Den wirksamen Einsatz der Verfahren zur Risikobewertung in einer gegebenen Situation, zur Ermittlung aktueller und zukünftiger Sicherheitsgefährdungen, analysieren können

Frage #2 (3 Punkte)

Als Teil einer Risikobewertung sind Sie dafür verantwortlich sicherzustellen, dass neue, extern hinzugezogene Lieferanten mit den von der Regierung angeordneten Richtlinien für das Projekt übereinstimmen. Auf welchen der Stakeholder sollten Sie sich in erster Linie konzentrieren, um sicher zu stellen, dass Ihre Lieferanten diesen Richtlinien auch weiterhin entsprechen?

a) Kunden, Benutzer und Lieferanten, um eine gute Kommunikation zwischen diesen sicherzustellen

b) Benutzer und Lieferanten, die sich nach aktueller Informationslage an das Gesetz halten

c) Bundesweite, landesweite und örtliche Behörden, die die zu befolgenden Richtlinien kommunizieren

d) Interne und externe Quellen, die die Informationen für weitere Risikoanalysen nutzen

C ist richtig, da das die Quelle der Richtlinien ist. Da sich diese Richtlinien jederzeit verändern können, ist es wichtig, immer auf dem neuesten Stand zu bleiben. A, B und D müssen ebenso informiert bleiben. Diese Informationen müssen aber von den bundesweiten, landesweiten und örtlichen Behörden kommen.

AS-1.2.1 (K2) Das Konzept der Sicherheitsrichtlinien und -verfahren sowie deren Anwendung in Informationssystemen verstehen

Frage #3 (1 Punkt)

Welcher der folgenden Punkte ist eine Konsequenz aus einer Richtlinie, die den Zugriff auf ein System oder Gerät auf ein akzeptables Level minimiert?

a) Weitere Geräte werden hinzugefügt, um die Auswirkungen zu mildern

b) Angemessene Kontrollen von selbst-versorgenden Geräten wie Router werden verboten sein

c) Geräte, die den Richtlinien nicht entsprechen, werden aus dem kabellosen Netzwerk entfernt

d) Zugriff auf VPN wird streng eingeschränkt werden

C ist richtig. Wenn eine solche Richtlinie eingeführt wird, werden Geräte, die der Richtlinie nicht entsprechen, so lange entfernt, bis sie angepasst sind. A ist falsch, da dies kein erwartetes Ergebnis wäre. B ist nicht richtig, da diese Kontrollen gefördert werden. D ist nicht korrekt, da der Zugriff nicht wie in D beschrieben streng eingeschränkt, sondern lediglich kontrolliert wird.

AS-1.2.2	(K4) Einen gegebenen Satz von Sicherheitsrichtlinien und -verfahren analysieren sowie die Ergebnisse von Sicherheitstests zur Ermittlung der Wirksamkeit bewerten können

Frage #4 (3 Punkte)

In Ihrer Rolle als Sicherheitsadministrator ist es Ihre Aufgabe, Ihrer Organisation zu helfen, die Effektivität von Sicherheitsrichtlinien und -verfahren innerhalb der gesamten Firma zu verstehen. Sie werden nach Fertigstellung der Analyse Ihre Ergebnisse zur Effektivität dem oberen Management berichten. Welcher der folgenden Punkte ist die optimale Strategie, um dies zu tun?

a) Eine Bewertung einer statischen Analyse jeweils unabhängig für Richtlinien und Vorgänge durchführen

b) Die Ergebnisse eines Sicherheitstests analysieren, um die Effektivität zu bestätigen

c) Die Ergebnisse von Sicherheitstests bewerten, bei denen der Schwerpunkt auf aktuellen Gefahren und Attacken liegt

d) Die statischen Testergebnisse für neue Softwaregefahren bewerten

B ist richtig. Sie sollten die Ergebnisse eines Sicherheitstests analysieren, um zu überprüfen, ob Richtlinien und Verfahren eingehalten werden und effektiv sind. A ist nicht richtig, da sich die statische Analyse – wenn überhaupt - auf den Code beziehen sollte. C ist nicht richtig, da der Schwerpunkt nicht nur auf den momentanen Gefahren und Attacken liegen sollte, sondern auch auf Konfigurationen etc. D ist nicht richtig, da der Schwerpunkt nicht nur auf entstehenden Gefahren liegt.

AS-2.2.1	(K2) Die Notwendigkeit von Sicherheitstests in einem Unternehmen verstehen können – einschließlich der Vorteile für das Unternehmen, wie bspw. die Risikominderung sowie größeres Vertrauen
AS-2.3.1	(K2) Den Einfluss von Projektrealitäten, geschäftlichen Einschränkungen, Softwareentwicklungslebenszyklen und anderen Überlegungen für die Aufgabe des Sicherheitstestteams analysieren und verstehen können

Frage #5 (1 Punkt)

Wie kann Sicherheitstesten für eine Organisation, die bei einer Verletzung der Sicherheit mit rechtlichen Konsequenzen zu rechnen hat, hilfreich sein?

a) Es kann zeigen, dass die Organisation mit angemessener Sorgfalt versucht hat, solche Vorkommnisse zu vermeiden

b) Die Dokumentation des Sicherheitstestens kann von Nutzen sein, um den Täter ausfindig zu machen

c) Da alle wichtigen Informationen vor Beginn der Sicherheitstests auf einem Backup (Sicherungskopie) gespeichert werden, kann dieses Backup genutzt werden, um alle beschädigten Informationen wiederherzustellen

d) Durch das Nachvollziehen der dokumentierten Tests kann das Sicherheitstestteam herausfinden, wie die Sicherheitsverletzung möglich war

A ist laut Lehrplan richtig. B ist nicht richtig, da diese Informationen wahrscheinlich nicht hilfreich sein werden. C ist nicht richtig, da Backups sehr wahrscheinlich nicht aktuell genug wären. Außerdem liegt nicht zwingend eine Veränderung der Daten vor. Das Problem besteht vermutlich eher im Bereich gestohlener oder fälschlich eingesehener Daten. D ist nicht richtig, da es zwar bestimmte Bereiche, in denen nicht genug getestet wurde, aufzeigen kann, es wird jedoch kaum bei der Verteidigung der Organisation bei rechtlichen Folgen helfen.

AS-2.4.1 (K2) Erläutern können, warum Ziele von Sicherheitstests an der Sicherheitsrichtlinie des Unternehmens und anderen Testzielen im Unternehmen ausgerichtet sein müssen

AS-2.4.3 (K2) Den Zusammenhang zwischen Informationsschutz und Sicherheitstesten verstehen

Frage #6 (1 Punkt)

Welche der folgenden Aussagen ist richtig?

a) Informationsschutz ist ein Teil des Sicherheitstestens

b) Informationsschutz und Sicherheitstesten sind zwei Ausdrücke, die das gleiche meinen

c) Sicherheitstesten ist ein Teil von Informationsschutz

d) Die zwei Ausdrücke beziehen sich auf unterschiedliche Bereiche von Sicherheit

C ist richtig. Sicherheitstesten ist ein Teil eines größeren Bereiches von Informationsschutz.

AS-2.4.2	(K3) Die Fähigkeit besitzen, Sicherheitstestziele auf der Grundlage von Funktionalität, Technologiemerkmalen und bekannten Schwachstellen, für ein gegebenes Projektszenario, auswählen zu können

Frage #7 (2 Punkte)

Sie arbeiten bei einer Bank als Teil des Sicherheitstestteams. Während eines kürzlich durchgeführten Sicherheitsaudits wurde bemerkt, dass die Passwörter der Benutzer nicht sicher genug sind. Seither wurde eine Reihe von neuen Anforderungen für die Sicherheit von Passwörtern herausgegeben. Was wäre unter diesen Umständen eine angemessene Auswahl von Sicherheitszielen zum Testen von allgemeinen Passwortregeln?

1) Verifizieren, dass die Passwörter den Voraussetzungen zur Länge entsprechen
2) Verifizieren, dass die Passwörter den Voraussetzungen zum Nutzen von Zeichen, Nummern, Buchstaben und Großschreibung entsprechen
3) Verifizieren, dass die Passworteingabe dreimal versucht werden kann
4) Verifizieren, dass die Passwörter nicht innerhalb eines Zeitraums von einem Jahr wiederverwendet werden können
5) Verifizieren, dass die Passwörter alle drei Monate neu vergeben werden müssen
6) Verifizieren, dass der Benutzer anfragen kann, das Passwort per Email zugesendet zu bekommen
7) Verifizieren, dass der Systemadministrator ein gesperrtes Passwort zurücksetzen kann

a) 1, 2, 3, 4 wahr 5, 6, 7 falsch

b) 1, 2, 4, 5 wahr 3, 6, 7 falsch

c) 3, 4, 6, 7 wahr 1, 2, 5 falsch

d) 4, 5, 6, 7 wahr 1; 2; 3 falsch

B ist richtig, da 1), 2), 4) und 5) stichhaltige Sicherheitsziele darstellen. A ist nicht richtig, da 3) eher funktional als sicherheitsrelevant ist (es sei denn, der Benutzer wird nach dreimaliger Passworteingabe gesperrt, aber das ist anhand der Beschreibung nicht erkennbar). C und D sind nicht richtig, da 6) und 7) eher funktional, also keine spezifischen Sicherheitsvoraussetzungen, sind.

AS-2.5.1	(K3) Die Fähigkeit besitzen, den Zusammenhang zwischen Sicherheitstestzielen und der Notwendigkeit einer starken Integrität von sensiblen digitalen und physischen Assets, für ein gegebenes Projektszenario, definieren zu können

Frage #8 (2 Punkte)

Ihre Firma war neulich in den Schlagzeilen, nachdem eine Sicherheitsverletzung dazu führte, dass vertrauliche Nutzerinformationen gestohlen wurden. Das Management reagierte damit, den Umfang des Sicherheitstestens sofort auszuweiten. Sie stimmen zwar zu, dass etwas getan werden muss, sind aber trotzdem beunruhigt, dass dieser Ansatz zu reaktionsfreudig ist und nicht in dem Testen resultiert, das eigentlich nötig wäre.

Welche Sorgen sind entlang des Lehrplans berechtigt, wenn diese Initiative eingeführt wird?

a) Beim Testen werden weiterhin Probleme übersehen, da es nicht ausreichend fokussiert sein wird

b) Das Testen wird ausgelagert (Outsourcing), so dass es effizienter wird

c) Der Bereich des Testens könnte zu groß werden und die adäquaten Ressourcen, um das auszugleichen, könnten fehlen

d) Die Ziele des Testens sind nicht klar genug definiert und könnten die gleichen Probleme übersehen, die bereits in der Produktion übersehen worden sind

C ist laut Lehrplan richtig, da dies ein weit verbreitetes Problem im Zusammenhang mit einer umfangreicheren Zieldefinition ist. A und D sind angemessene Bedenken. Da wir aber nicht wissen, wann oder wie die Testziele definiert werden, könnte das trotzdem kontrollierbar sein. B ist immer eine Möglichkeit und könnte auch hier die richtige Handlungsweise sein. Da es aber keinen Hinweis darauf gibt, dass Outsourcing zu diesem Zeitpunkt vorgenommen wird, ist die Antwort nicht richtig.

AS-2.6.1	(K4) In einer gegebenen Situation ermitteln können, welche Sicherheitstestvorgehensweisen wahrscheinlich am erfolgreichsten sind
AS-2.6.2	(K4) Analyse einer Situation, in der eine gegebene Sicherheitstestvorgehensweise fehlgeschlagen ist und Ermittlung der wahrscheinlichen Ursachen für das Fehlschlagen
AS-2.7.1	(K4) Die Hauptleistungsindikatoren (KPIs) zur Ermittlung von Sicherheitstestpraktiken mit und ohne Optimierungsbedarf analysieren können

Frage #9 (3 Punkte)

Für eine Firma, die sensible medizinische Informationen, die zwischen Ärzten und Krankenhäusern geteilt werden, verarbeitet, haben Sie die Aufgabe übernommen, ein Sicherheitstestteam zu gründen. Sie haben festgestellt, dass die Sicherheit bezüglich dieser medizinischen Informationen nicht ausreicht, um sie vor versehentlicher Enthüllung oder sogar Hackern zu schützen. Die Person, die vorher Ihren Job gemacht hat, hat eine Reihe von Beratern für das Testen eingestellt. Die Testergebnisse wurden jedoch nicht dokumentiert und es wurde nichts geändert. Um genau zu sein, kennen Sie noch nicht einmal die Abdeckung der Tests. Sie haben Ihre Ergebnisse der Unternehmensleitung vorgestellt. Diese hat zwar zugestimmt, dass Sicherheitstesten prinzipiell benötigt wird, sie hat Ihnen jedoch weder Zeit noch Budget dafür zur Verfügung gestellt. Es scheint so, als wüsste die Unternehmensleitung zwar, dass ein größerer Fokus auf das Thema Sicherheit gut wäre, gleichermaßen ist sie aber nicht über die Folgen im Bilde, die damit einhergehend unternommen werden müssten. Was sollte Ihr erster Schritt sein, um die Unternehmensleitung an die zu erledigende Arbeit heranzuführen?

a) Eine detaillierte Liste mit allen möglichen Sicherheitslücken erstellen und der Unternehmensleitung präsentieren

b) Eine Zusammenfassung Ihrer Teststrategie zur Verfügung stellen und Beispiele geben, wie das Testen geleitet werden kann

c) Die Rechtsabteilung hinzuziehen, um zu erklären, wieviel die Sicherheitsverletzungen das Unternehmen kosten könnten

d) Eine Sicherheits- und Sicherheitstestrichtlinie entwickeln, um so zu zeigen, wie diese in Einklang mit Ihrer Teststrategie steht

D ist richtig. Zu diesem Zeitpunkt braucht die Organisation eine Richtlinie und einen Plan auf Management Level, um weiter zu kommen. Ohne diese Richtlinie ist das Testen weiterhin nur sporadisch. Außerdem wird es sonst schwierig werden, finanzielle Unterstützung und den Rückhalt von Seiten des Managements zu bekommen. A und C sind zu diesem Zeitpunkt nicht richtig. Sie könnten erst nützlich werden, wenn während der Implementierung der Richtlinie Schwierigkeiten mit der Finanzierung aufkommen sollten. B ist nicht richtig, da Sie eine übergreifende Richtlinie brauchen, bevor Sie den Lösungsansatz festlegen können.

AS-2.6.3	(K3) Die Fähigkeit besitzen, für ein gegebenes Projektszenario verschiedene Stakeholder zu ermitteln und den Nutzen des Sicherheitstestens für jede Stakeholdergruppe zu veranschaulichen

Frage #10 (2 Punkte)

Sie kommen gerade von einem Treffen, bei dem über die Sicherheitsvorgehensweise der Organisation diskutiert wurde. Ein besonders bedeutungsvoller Punkt war die Wichtigkeit des Testens, um sicher zu gehen, dass Daten vor betrügerischem Zugriff geschützt sind, insbesondere Kreditkarteninformationen. Sie wurden gebeten, eine Reihe von Testzielen vorzubereiten, die helfen sollen, die Risikobereiche einzugrenzen. Eine Ihrer Aufgaben ist es, sicherzustellen, dass alle Bedenken der Stakeholder aufgegriffen werden. Welche Gruppe von Stakeholdern wird am wahrscheinlichsten den Vorteil Ihrer Arbeit sehen?

a) Unternehmensleitung

b) Compliance-Beauftragte

c) Geschäftskunden

d) Zuständige aus dem regulatorischen Bereich

C ist richtig. Da die Daten von Geschäftskunden angreifbar sind, werden sie sich als erstes Sorgen um betrügerische Attacken machen. Man würde hoffen, dass A, B und D auch eingebunden werden. Dies passiert aber meist nicht im ersten Schritt.

AS-3.1.1	(K3) Die Elemente eines wirksamen Sicherheitstestprozesses für ein gegebenes Projekt definieren können

Frage #11 (2 Punkte)

Als Sicherheitsadministrator sind Sie für Aspekte des Sicherheitsprozesses (inklusive Testen) verantwortlich. Für diesen Prozess nutzen Sie logische Tests (abstrakt) als Grundlage für manuelle Tests, um diese aus Sicht des externen Lieferanten durchzuführen. Welcher Sicherheitstestprozess ist am besten geeignet, um dies parallel durchzuführen?

a) Sicherheitstestentwicklung auf Basis von Bedingungen und Zielen

b) Sicherheitstestimplementierung

c) Allumfassende Bewertungen und Berichte des Sicherheitstestens

d) Sicherheitstestanalyse und Entwurf

B ist richtig. Das Nutzen von logischen Tests zum Entwerfen von manuellen Tests und deren Ausführung ist Teil der Sicherheitstestimplementierung. A und D sind nicht richtig, da dies schon bei dem Entwurf des logischen Tests erledigt wurde. C ist erst nach der Durchführung der Tests relevant.

AS-3.2.1	(K4) Eine Sicherheitstestvorgehensweise sowie deren Stärken und Schwächen analysieren und erläutern können

Frage #12 (3 Punkte)

Sie haben einen Sicherheitstestplan für ein System entwickelt, welches medizinische Informationen für Kunden speichert und die Daten an den jeweiligen Arzt weiterleitet. Sie haben folgende Bereiche in Ihrem Sicherheitstestplan abgedeckt:

- Geltungsbereich (was ist innerhalb des Geltungsbereichs, was ist außerhalb des Geltungsbereichs)
- Rollen und Aufgaben
- Verantwortlichkeiten (Lieferanten vs. Intern)
- High-level Zeitplan
- Umgebungsanforderungen und -aufbau
- Liste notwendiger Autorisierungen und Genehmigungen

Welche Informationen müssen Sie noch für diesen Sicherheitstestplan bereitstellen, um das Minimum an Anforderungen, wie im Lehrplan beschrieben, zu erreichen?

a) Eine Liste der notwendigen Zugangsdaten und Trainings für die Tester

b) Einen Zeitplan, der die Zeit für Design, Ausführung und Bewertung des Sicherheitstests enthält

c) Eine Kopie der behördlichen Standards, die vom System eingehalten werden müssen

d) Eine Liste der Personen und ihrer Kontaktdaten, die das Testen durchführen, für den Fall, dass eine Sicherheitsverletzung vorkommt

B ist laut Lehrplan richtig. A könnte nötig sein, ist aber keine Minimalanforderung und könnte schon in dem Abschnitt über Rollen und Verantwortlichkeiten enthalten sein. C ist nicht richtig, da Standards im Plan nicht enthalten sind und somit auch keine Kopie vorliegen kann. D ist nicht richtig, da solche Details nicht im Plan enthalten sein sollten. Ferner ist es zu vermeiden/unterlassen, einzelne Tester wegen solcher Verstöße direkt zu kontaktieren.

AS-3.3.1	(K3) Für ein gegebenes Projekt auf der Grundlage einer gegebenen Sicherheitstestvorgehensweise und unter Berücksichtigung funktionaler und struktureller Sicherheitsrisiken logische (abstrakte) Sicherheitstests realisieren können
AS-3.3.2	(K3) Testfälle zur Validierung von Sicherheitsrichtlinien und -verfahren realisieren können

Frage #13 (2 Punkte)

Welcher der folgenden Testfälle testet das Sicherheitsvorgehen eines Systems am geeignetsten?

a) Drei gescheiterte Login-Versuche erzeugen eine Nachricht „Gesperrt“. Kontaktieren Sie Ihren Manager oder Systemadministrator, so dass Ihnen ein temporäres Passwort via Telefon gegeben werden kann. Dann müssen Sie das temporäre Passwort beim Einloggen wieder ändern. Sie loggen sich aus und dann mit dem neu erstellten Passwort wieder ein.

b) Nach mehreren Login-Versuchen bekommen Sie eine Nachricht über Ihre Sperrung. Sie rufen die IT-Betreuung an, um ein neues Passwort zu erhalten. Dann loggen Sie sich mit dem temporären Passwort ein, loggen sich anschließend aus und erstellen beim erneuten Login Ihr neues Passwort.

c) Nach mehreren Versuchen werden Sie vom System gesperrt. Sie nutzen ein Passwort, das zuvor funktionierte, jetzt jedoch nicht mehr funktioniert. Sie versuchen ein neues Passwort zu erstellen, obwohl Sie nun gesperrt sind. Ein kompletter Neustart der Maschine ist der nächste Schritt, um zur erneuten Eingabe des Passworts zu gelangen.

d) Nach dem ersten Versuch, ein ungütiges Passwort einzugeben, nutzen Sie direkt eine Liste von Passwörtern Ihres PCs, um sicher zu gehen, dass Sie das Richtige nutzen. Sie probieren ein anderes Passwort der Liste aus und es funktioniert sofort.

A ist richtig. B und C sind aufgrund des Wortes „mehrere“ nicht richtig. D ist nicht richtig, da dies sicher kein gutes Sicherheitsvorgehen ist.

AS-3.4.1	(K2) Schlüsselelemente und Merkmale einer effektiven Sicherheitstestumgebung verstehen
AS-3.6.1	(K2) Die Bedeutung der Wartung von Sicherheitstestprozessen vor dem Hintergrund der Weiterentwicklung von Technologie und Gefährdungen verstehen

Frage #14 (1 Punkt)

Welche der folgenden Auswahlmöglichkeiten ist ein Hauptmerkmal einer effektiven Sicherheitstestumgebung?

a) Enge Anbindung an das Produktionssystem, um die Sicherheit an jedem Punkt zu garantieren

b) Isolierung von unterschiedlich alten Versionen des Betriebssystems in der Testumgebung

c) Abbildung der Produktionsumgebung in Hinblick auf die Zugriffsrechte

d) Vorhalten aller Plug-Ins der Produktionsumgebung sowie aller nicht in der Produktionsumgebung enthaltenen Plug-Ins, um ein verständliches Aufsetzen sicher zu stellen

C ist richtig, denn je näher die Testumgebung der Produktionsumgebung ist, desto realistischer wird das Testen sein. Dies gilt besonders, wenn es um Zugriffsrechte und Delegationseinstellungen geht. A ist nicht richtig, da die Systeme nicht angebunden sein müssen und auch nicht sein sollten. B könnte hilfreich sein, ist aber kein Hauptmerkmal. D ist nicht richtig, da es Plug-Ins enthält, die nicht in der Produktion enthalten sind, was sowohl zu falsch positiven als auch zu falsch negativen Ergebnissen führen könnte.

AS-3.4.2	(K2) Die Bedeutung der Planung und Einholung von Genehmigungen vor der Durchführung jedes Sicherheitstests verstehen

Frage #15 (1 Punkt)

Welche Herausforderung erwartet Sie, wenn Sie eine Genehmigung für Sicherheitstestwerkzeuge einholen sollen?

a) Einige Länder verbieten das Nutzen bestimmter Sicherheitstestwerkzeuge

b) Der Genehmigungsprozess für Sicherheitstestwerkzeuge auf Basis einer Ausnahme muss überbrückt werden können, falls bösartige Vorkommnisse passieren

c) Die Risiken eines Werkzeuges sind selten bekannt, bevor dieses bereitgestellt wird, und sie sind besser zu erkennen, wenn es bereits genutzt wird

d) Es sind keine vorbeugenden Maßnahmen nötig, da Risiken von Sicherheitstestwerkzeugen normalerweise unbekannt sind

A ist richtig. Obwohl einige Werkzeuge gut und effektiv zum Testen genutzt werden können, können sie in einigen Ländern und Organisationen verboten sein. B ist nicht richtig, da immer die Gefahr besteht, ein suboptimales Werkzeug zum Lösen einer Krise einzusetzen. Eine schnelle Genehmigung macht Sinn, aber eine komplette Überbrückung ist risikoreich. C und D sind nicht richtig, da es unbekannte Risiken von Werkzeugen geben könnte und es besser ist, eine sorgfältige Prüfung bei der Auswahl des Werkzeugs vorzunehmen, als mit den Konsequenzen eines schlecht ausgewählten Werkzeuges umgehen zu müssen.

AS-3.5.1 (K4) Sicherheitstestergebnisse für die Ermittlung folgender Punkte analysieren können:

- Art der Sicherheitsschwachstelle
- Ausmaß der Sicherheitsschwachstelle
- Potenzielles Schadensausmaß der Sicherheitsschwachstelle
- Vorgeschlagene Abhilfemaßnahmen
- Optimale Testberichtsmethoden

Frage #16 (3 Punkte)

Nach einem Update und den dazugehörigen Tests Ihrer eCommerce-Seite bewerten Sie einen Satz von Sicherheitstestergebnissen, bevor Sie die aktualisierte Seite für die Produktion freigeben. Sie stellen fest, dass die Applikation einen Fehler enthält, der Cross-Site-Scripting möglich macht. Welche der folgenden Möglichkeiten enthält die richtigen Dinge, die nun getan werden sollten?

a) Das Problem einem Entwickler melden, es dem Bericht für die Stakeholder hinzufügen und weiter testen, um weitere Fehler festzustellen

b) Testen, ob das Problem ebenfalls in der aktuellen Version besteht, den Fehler in einem sicheren System dokumentieren, einen Entwickler benachrichtigen und weiterhin auf weitere XSS Fehler testen

c) Das Ausmaß des Problems untersuchen, indem weitere Tests an dem freizugebenden Produkt durchgeführt werden. Besonderer Schwerpunkt sollte auf XSS Problemen und der Durchführung einer Analyse des Codes liegen

d) Das Management informieren, den Defekt dokumentieren und in Ihrem wöchentlichen Bericht der Stakeholder festhalten, weiterhin auf andere Sicherheitsdefekte testen, um das Ausmaß der Sicherheitsprobleme festzustellen

B ist richtig. Es ist oberste Priorität, festzustellen, ob das Problem in der Produktionsversion ebenfalls besteht. Die Fehler sollten in einem sicheren Dokument zur Fehlerverfolgung festgehalten werden, da sie ebenfalls in der Produktionsversion bestehen könnten. Da bereits ein XSS Problem festgestellt wurde, könnte es noch mehr geben, daher ist es sinnvoll, weiterhin zu testen. A ist nicht richtig, da der Fehler nicht im Stakeholder Bericht publiziert werden sollte. C ist nicht richtig, da weiteres Testen zwar nötig ist, die besondere Kritikalität aber auf der Benachrichtigung liegt. D ist nicht richtig, da wie in A der Fehler nicht im Stakeholder Bericht aufgeführt werden sollte.

AS-4.1.1	(K2) Erläutern können, warum sich Sicherheit am besten innerhalb eines Lebenszyklusprozesses erreichen lässt

Frage #17 (1 Punkt)

Zu welchem Zeitpunkt im Softwareentwicklungslebenszyklus sollte überprüft werden, dass sichere Programmierpraktiken verwendet wurden?

a) Komponententest

b) Integrationstest

c) Systemtest

d) Sicherheitsabnahmetest

A ist richtig. Das Überprüfen sollte zeitgleich zum Schreiben des Codes stattfinden.

AS-4.1.2	(K3) Die entsprechenden, sicherheitsbezogenen Aktivitäten für einen gegebenen Softwareentwicklungslebenszyklus (z.B. iterativ, sequenziell) realisieren können

Frage #18 (2 Punkte)

Ein Unternehmensanalyst hat Sie beauftragt, die Anforderungen für die Sicherheitsaspekte eines Systems neu zu definieren. Es geht um ein sicherheitskritisches System, das medizinische Informationen für Patienten speichert und diese an Gesundheitsspezialisten in Krankenhäusern, Arztpraxen oder Krankenwagen weitergibt. An welcher Stelle im Softwareentwicklungslebenszyklus sollten die Sicherheitsanforderungen dokumentiert und wie detailliert sollte dies getan werden?

a) Sie sollten gar nicht formal dokumentiert werden, da die Sicherheitsimplementierung innerhalb des Codes vor Außenstehenden zu schützen ist

b) Sie sollten während der Anforderungsphase in einer detaillierten und eindeutigen Art und Weise in den Anforderungsdokumenten festgehalten werden

c) Sie sollten während der Designphase (Programmieransatz bekannt) festgehalten werden und nicht in der Anforderungsphase (Programmieransatz noch nicht bekannt)

d) Sie sollten auf den funktionalen Zugriff und die Erreichbarkeit aus Sicht des Nutzers begrenzt werden und in der Anforderungsphase dokumentiert werden

B ist richtig. A ist nicht richtig, obwohl es wichtig ist, dass die dokumentierten Anforderungen vor jedem geschützt sind, der sie nicht kennen muss. C ist nicht richtig, da Anforderungen in der Designphase zwar weiterentwickelt werden können, aber in der Anforderungsphase bereits initial festgehalten werden sollten. D ist nicht richtig, da Sicherheitsanforderungen ebenfalls sichere Programmierpraktiken etc. enthalten sollten.

AS-4.2.1	(K4) Einen gegebenen Satz von Anforderungen aus der Sicherheitsperspektive analysieren können, um Unzulänglichkeiten zu ermitteln
AS-4.3.1	(K4) Ein gegebenes Entwurfsdokument aus der Sicherheitsperspektive analysieren können, um Unzulänglichkeiten zu ermitteln

Frage #19 (3 Punkte)

In der Produktion wurde eine Unzulänglichkeit gefunden. Wenn ein unautorisierter Nutzer eine URL von einer Websession eines autorisierten Nutzers kopiert, kann der unautorisierte Nutzer diese URL in seine Sitzung einfügen und mit den Rechten des autorisierten Nutzers fortfahren. In diesem Fall wurde berichtet, der unautorisierte Nutzer hätte die URL des autorisierten Nutzers verwenden können, um das Passwort der Systemadministration zu ändern. Um diese Lücke zu schließen, wollen die Entwickler die ID der Sitzung und die ID des Nutzers, wann immer eine URL verwendet wird, überprüfen.

Welche Befürchtung ist bei dieser Lösung realistisch?

a) Es wird das Problem nicht lösen, da das Hijacken von Sitzungen weiterhin möglich sein wird

b) Es wird das Problem lösen, aber die Benutzbarkeit könnte nachteilig beeinflusst werden

c) Es wird das Problem lösen, aber die Leistung könnte nachteilig beeinflusst werden

d) Es wird das Problem nicht lösen, sondern lediglich neue Angriffspunkte durch die Sitzungs-IDs eröffnen

C ist richtig. Es ist sehr wahrscheinlich, dass eine Überprüfung auf dieser Ebene das System verlangsamen wird, da die Überprüfung bei jedem Seitenwechsel stattfinden müsste. A und D sind nicht richtig, da es in der Frage um eine „Lösung“ geht, diese beiden Antworten aber davon ausgehen, dass das Problem nicht gelöst wird. B ist nicht richtig, da die Benutzbarkeit nicht eingeschränkt werden sollte (außer Sie sind der Hacker!).

AS-4.4.1 (K2) Die Rolle des Sicherheitstestens beim Komponententest verstehen

AS-4.4.4 (K2) Die Rolle des Sicherheitstestens beim Komponentenintegrationstest verstehen

Frage #20 (1 Punkt)

Wieso sollten Sicherheitstester die Compiler-Warnungen während eines Tests auf Komponentenebene beachten?

a) Weil diese auf Sicherheitsprobleme hinweisen, die repariert werden müssen

b) Weil diese auf potenzielle Probleme hinweisen, die untersucht werden sollten

c) Weil diese auf Programmierfehler hinweisen, die wiederum funktionale Fehler verursachen werden

d) Weil diese auf schlechte Programmierpraktiken hinweisen, die vermehrte Wartbarkeit nach sich ziehen werden

B ist richtig. Vom Standpunkt eines Sicherheitstesters können Compiler-Warnungen auf potenzielle Gefahren hinweisen, die zu Sicherheitslücken führen könnten. A ist nicht richtig, da Warnungen nicht zwingend eine Reparatur benötigen. C und D können zwar richtig sein, sind aber nicht relevant für das Sicherheitstesten.

AS-4.4.2	(K3) Sicherheitstests auf Komponentenebene (abstrakt) bei einer definierten Spezifikation realisieren können
AS-4.4.5	(K3) Komponentenintegrationssicherheitstests (abstrakt) bei einer definierten Systemspezifikation realisieren können

Frage #21 (2 Punkte)

Sie haben ein System getestet, das 20 definierte Komponenten hat. Sie haben umfangreiche Sicherheitstests an jeder Komponente durchgeführt. Das System ist nun bereit, zum Sicherheitstesten der Komponentenintegration überzugehen. Wie sollten Sie diese Tests angehen?

a) Da sich Komponentenintegrationstests mit der Summierung von Angriffspunkten der verschiedenen Komponenten befassen, ist es das Beste, die gleichen Tests an den integrierten Komponenten durchzuführen.

b) Das Hauptrisiko ist die Integration der Komponenten. Daher sollte jede Verbindung einzeln getestet und verifiziert werden, so dass es keine fehlerhaften Verbindungen gibt. Die Komponenten selbst sollten ebenfalls erneut getestet werden.

c) Es ist wahrscheinlich, dass neue Angriffspunkte sowohl durch die integrierten Komponenten als auch durch die Möglichkeit, das größere System und die Infrastruktur zu betreiben, aufgetreten sind. Um nun auch diese Bereiche abzudecken, sollte das Testen um diese Aspekte ausgeweitet werden.

d) Da die Komponenten nun integriert und die möglichen Interaktionen begrenzt sind, sollten die Sicherheitsrisiken reduziert sein. Daher sollten nur die Integrationspunkte getestet werden. Ein erneutes Testen der Komponenten ist folglich nicht nötig.

C ist richtig. Mit integrierten Komponenten können neue Angriffspunkte auftreten und wahrscheinlich neue Testbereiche zur Verfügung stehen. A ist nicht richtig, da Komponentenintegrationstests nicht die Summe der einzelnen Komponenten sind. B ist nicht richtig, da das Testen nicht auf die Verbindungen und ursprünglichen Komponenten begrenzt werden sollte. D ist nicht richtig, da Sicherheitsrisiken in integrierten Systemen eher vermehrt auftreten.

AS-4.4.3 (K4) Ergebnisse eines gegebenen Tests auf Komponentenebene analysieren können, um die Angemessenheit von Programmcode aus der Sicherheitsperspektive zu ermitteln Frage #22 (3 Punkte)

Sie erstellen Sicherheitstestfälle für eine SQL-Injection über ein Eingabefeld, in dem bis zu 5 alpha-numerische Zeichen erlaubt sind. Dabei unterteilen Sie die Testfälle in Äquivalenzklassen, um deren Anzahl zu reduzieren. Welche der folgenden Möglichkeiten enthält die minimale Auswahl von Eingaben, die Sie, unter Berücksichtigung dieser Informationen, testen sollten?

a) bbbbb, 12345, ‘

b) %, ‘, @, ab123

c) ‘, ab123

d) ‘

C ist richtig, denn es enthält einen Test für SQL-Injection und einen für eine gültige Eingabe. Somit ist das Minimum an Tests erreicht. A und B haben mehr als das gefragte Minimum und D enthält nicht genügend Testfälle, da es nicht die gültige Eingabe testet. Es ist ratsam, zusätzliche Tests, die die SQL-Injection abfragen, hinzuzufügen. Allerdings wird bei dieser Frage die Verwendung von Äquivalenzklassen verlangt und nach dem Minimum gefragt.

AS-4.5.1	(K3) Ende-zu-Ende-Testszenarien, die eine oder mehrere Sicherheitsanforderunge(n) verifizieren und einen beschriebenen funktionalen Ablauf testen, für Sicherheitstests realisieren können
AS-4.6.1	(K3) Eine durchgängige Vorgehensweise für Sicherheitswiederholungs- bzw. Regressionstests auf der Basis eines gegebenen Szenarios realisieren können

Frage #23 (2 Punkte)

An Sie wurden folgende Anforderungen für das Sicherheitstesten gestellt.

Nutzer haben die Möglichkeit, ihr Passwort abzufragen. Wenn solch eine Anfrage gestellt wird, müssen zwei der drei Sicherheitsfragen des Nutzers richtig beantwortet werden. Sind die Antworten richtig, wird ein Link an die hinterlegte Email-Adresse gesendet. Dieser Link verweist auf eine Seite, auf der das Passwort zurückgesetzt werden kann. Sobald dies erledigt ist, kann das neue Passwort zum Einloggen verwendet werden. Eine Stunde nach dem Versenden muss der Link deaktiviert werden. Die Nutzer dürfen nur zwei Anfragen für ein neues Passwort stellen, ohne ein Zurücksetzen herbeizuführen. Ansonsten müssen sie den Helpdesk anrufen. Bei jedem anderen Fehler wird die Nutzer ID gesperrt und muss vom Helpdesk entsperrt werden.

Welche der folgenden Möglichkeiten enthält die Minimalanforderungen für die Testbedingungen, um die funktionale Sicherheit adäquat zu testen?

a) Ungültiger Nutzer; gültiger Nutzer; 2 richtige Antworten; 2 falsche Antworten; gültige Email-Adresse; ungültige Email-Adresse; zurücksetzen mit gültigem Passwort; zurücksetzen mit ungültigem Passwort; Link gültig; Link abgelaufen; zwei Anfragen ohne Zurücksetzen; drei Anfragen ohne Zurücksetzen

b) Gültiger Nutzer; 2 richtige Antworten; gültige Email-Adresse, Zurücksetzen mit gültigem Passwort; Link gültig; zwei Anfragen ohne Zurücksetzen

c) Ungültiger Nutzer; 2 falsche Eingaben; ungültige Email-Adresse; Zurücksetzen mit ungültigem Passwort; Link abgelaufen; drei Anfragen ohne Zurücksetzen

d) Buffer Overflow in jedem Eingabefeld; SQL-Injection in jedem Eingabefeld; XXS auf der Seite des Logins und Passwort Zurücksetzens; ungültiger Nutzer; gültiger Nutzer; 2 richtige Antworten; 2 falsche Antworten; gültige Email-Adresse; ungültige Email-Adresse; Zurücksetzen mit gültigem Passwort; Zurücksetzen mit ungültigem Passwort; Link gültig; Link abgelaufen; zwei Anfragen ohne Zurücksetzen; drei Anfragen ohne Zurücksetzen

A ist richtig, da es die Hauptszenarios für die in den Anforderungen genannte funktionale Sicherheit abdeckt. B testet nur gültige Tests und C testet nur die Fehlerbedingungen. D beinhaltet sowohl Tests für Angriffe als auch funktionale Tests.

AS-4.5.2 (K3) Einen Satz von Abnahmekriterien für die Sicherheitsaspekte eines gegebenen Abnahmetests definieren können

Frage #24 (2 Punkte)

Nutzer haben die Möglichkeit, ihr Passwort abzufragen. Wenn solch eine Anfrage gestellt wird, müssen zwei der drei Sicherheitsfragen des Nutzers richtig beantwortet werden. Sind die Antworten richtig, wird ein Link an die hinterlegte Email-Adresse gesendet. Dieser Link verweist auf eine Seite, auf der das Passwort zurückgesetzt werden kann. Sobald dies erledigt ist, kann das neue Passwort zum Einloggen verwendet werden. Eine Stunde nach dem Versenden muss der Link deaktiviert werden. Die Nutzer dürfen nur zwei Anfragen für ein neues Passwort stellen, ohne ein Zurücksetzen herbeizuführen. Ansonsten müssen sie den Helpdesk anrufen. Bei jedem anderen Fehler wird die Nutzer ID gesperrt und muss vom Helpdesk entsperrt werden.

Welche der folgenden Möglichkeiten ist eine gültige Menge von Abnahmekriterien für diese Anforderungen?

1) Nutzer können ihr Passwort zurücksetzen, wenn weniger als drei Anfragen seit dem letzten Zurücksetzen gestellt und zwei Sicherheitsfragen richtig beantwortet wurden sowie der Link zum Zurücksetzen des Passworts genutzt und auf Anfrage ein gültiges Passwort angegeben wird
2) Mehr als zwei Anfragen führen zur Sperrung der Nutzer ID
3) Mehr als zwei Anfragen ohne Zurücksetzen führen zur Sperrung der Nutzer ID
4) Mehr als zwei misslungene Sicherheitsfragen führen zu einem Fehler
5) Mehr als zwei misslungene Sicherheitsfragen führen zur Sperrung der Nutzer ID
6) Wenn das System eine fehlerhafte Email-Adresse erhält, wird die Nutzer ID gesperrt
7) Wenn ein ungültiges Passwort beim Zurücksetzen eingegeben wird, werden dem Nutzer die Passwortvorgaben angezeigt
8) Ein Zurücksetzen des Passworts kann zum Einloggen in das System genutzt werden

a) 1, 2, 4, 6, 7, 8 wahr 3, 5 falsch

b) 1, 2, 3, 4, 5, 6, 7, 8 wahr

c) 3, 5, 6, 7, 8 wahr 1, 2, 4 falsch

d) 1, 3, 5, 6, 8 wahr 2, 4, 7 falsch

D ist richtig, da es die Abnahmekriterien enthält, die auf den Anforderungen basieren. 7 ist verlockend und logisch, wird aber nicht in der Anforderung aufgeführt. Die anderen Möglichkeiten sind nicht richtig, da sie nicht die richtigen Kriterien enthalten. 2 ist falsch, wohingegen 3 richtig ist. 4 ist falsch, wohingegen 5 richtig ist.

AS-5.1.1	(K2) Das Konzept der Systemhärtung und ihrer Rolle bei der Optimierung der Sicherheit verstehen
AS-5.1.2	(K3) Demonstrieren können, wie sich die Wirksamkeit allgemeiner Mechanismen der Systemhärtung testen lässt

Frage #25 (2 Punkte)

Um die Effektivität der Sicherheit eines Systems zu testen, implementieren Sie Verfahren zur Bewertung der Systemhärtung. Welches Verfahren würden Sie wählen, um sicher zu gehen, dass eingerichtete Mechanismen der Systemhärtung wie erwartet funktionieren?

a) Verschiedene Sicherheitsleistungsberichte und -metriken genau betrachten, um festzustellen, ob ein angemessenes Zugangs- und Authentifizierungslevel erlangt wurde.

b) Regelmäßige Überprüfung der Stabilität der Authentifizierung, um zu jeder Zeit einen hohen Schutz vor Eindringlingen zu garantieren

c) Bewertung der Hardware-Komponenten, die gehärtet wurden. Vergleich dieser Komponenten mit anderen gehärteten Software-Komponenten, um ein Gleichgewicht zu garantieren

d) Einen bekannten Hacker anwerben, um eine unabhängige Einschätzung zur Effektivität der Härtung zu erhalten

A ist richtig. Es sind Sicherheitsleistungsberichte und -metriken verfügbar, mit denen festzustellen ist, ob ein angemessenes Level an Härtung erreicht wurde. B ist nicht richtig, da stabile Authentifizierung nur einen Aspekt der Härtung darstellt. C ist nicht richtig, denn es wird kein Gleichgewicht benötigt. Die kritischen Bereiche könnten eine bessere Härtung benötigen. D ist nicht richtig, da die Gefahr besteht, dass der Hacker Ihnen nicht berichtet, was er findet.

AS-5.2.1	(K2) Den Zusammenhang zwischen Authentifizierung und Autorisierung verstehen sowie bei der Sicherung von Informationssystemen anwenden können
AS-5.2.2	(K3) Demonstrieren können, wie sich die Wirksamkeit allgemeiner Authentifizierungs- und Autorisierungsmechanismen testen lässt

Frage #26 (1 Punkt)

Was sind Schlüsselattribute einer Sicherheitsautorisierung eines mittelmäßig komplexen IT-Systems?

a) Sie verifiziert, dass der Nutzer das richtige Profil und die entsprechenden Rechte hat, um auf geschützte Bereiche des Systems zuzugreifen

b) Sie ist wichtig, um herauszufinden, wie viele Ressourcen des Systems der Nutzer verwenden darf

c) Sie verifiziert, dass Nutzer, die das System benutzen, berechtigt sind

d) Sie verwendet allgemein bekannte Anmeldedaten der Nutzer, um Eintritt in das System zu erlangen

C ist richtig. Es verifiziert, dass der Nutzer berechtigt und autorisiert ist. A ist nicht richtig, da es nicht die Zugangsrechte beachtet. B ist nicht richtig, da die Verwendung von Systemressourcen hier nicht berücksichtigt wird. D ist nicht richtig, da die Verifizierung von weit verbreiteten und bekannten Nutzeranmeldedaten nicht genutzt werden sollte. Jeder Nutzer sollte einmalige Anmeldedaten haben.

AS-5.3.1	(K2) Das Konzept der Verschlüsselung sowie deren Anwendung bei der Sicherung von Informationssystemen verstehen
AS-5.3.2	(K3) Demonstrieren können, wie sich die Wirksamkeit allgemeiner Verschlüsselungsmechanismen testen lässt

Frage #27 (2 Punkte)

Die typischen Verschlüsselungsmechanismen sind angreifbar, daher ist es wichtig, über ihre Effektivität zu jedem gegebenen Zeitpunkt Bescheid zu wissen. Welchen der folgenden Verschlüsselungsmechanismen sollten Sie implementieren, um Vertrauen zu erhalten?

a) Werten Sie kryptographische Schlüssel aus, um sicher zu gehen, dass sie mindestens eine Länge von 256 Bits haben

b) Stellen Sie sicher, dass Sie, wo immer Sie können, Zufallsalgorithmen verwenden, um zufällige Zahlen zu generieren

c) Entwickeln Sie Tests, die sicher stellen, dass symmetrische Verschlüsselung in den richtigen Modi verwendet wird

d) Alle WEP-Protokolle entfernen, um zu prüfen, wie das System funktioniert

C ist laut Lehrplan richtig. A ist nicht richtig, da ein Minimum von 768 Bits verwendet werden sollte. B ist nicht richtig, da der Zufallsalgorithmus einfach zu knacken ist. D ist nicht richtig, da WEP-Protokolle erhalten bleiben und nicht entfernt werden sollten.

AS-5.4.1	(K2) Das Konzept der Firewalls und den Einsatz von Netzwerkzonen sowie ihre Anwendung bei der Sicherung von Informationssystemen verstehen
AS-5.4.2	(K3) Demonstrieren können, wie sich die Wirksamkeit bestehender Firewall-Implementierungen und Netzwerkzonen testen lässt

Frage #28 (1 Punkt)

Welche der Aussagen über die Beziehung einer Firewall und einer Netzwerkzone ist wahr?

a) Sowohl eine Netzwerkzone als auch eine Firewall konzentriert sich auf die Größe der Daten, die hindurchfließen

b) Eine Netzwerkzone kommuniziert mit sicheren Protokolloptionen, während eine Firewall sicherstellt, dass diese Protokolle sicher sind

c) Ein Subnetzwerk kann als Netzwerkzone betrachtet werden und eine Firewall kann ein System zur Überwachung des Datenverkehrs sein

d) Eine Netzwerkzone blockiert bösartigen Verkehr mit einer nicht vertrauten Zone, die die Firewall nicht filtert

C ist laut Lehrplan richtig. A ist nicht richtig, da eine Netzwerkzone sich nicht auf die Größe der Daten konzentriert. B ist nicht richtig, da Netzwerkzonen ein Teil der Konfiguration einer Firewall sind und den autorisierten Datenstrom zwischen Netzwerken definieren. D ist nicht richtig, da eine Firewall, und nicht die Netzwerkzone, den Verkehr sperrt.

AS-5.5.1	(K2) Das Konzept der Angriffserkennungswerkzeuge sowie deren Anwendung bei der Sicherung von Informationssystemen kennen
AS-5.5.2	(K3) Demonstrieren können, wie sich die Wirksamkeit bestehender Angriffserkennungswerkzeuge testen lässt

Frage #29 (2 Punkte)

Sie arbeiten in einer Organisation, die ein Angriffserkennungssystem (IDS) einsetzt. Sie machen sich Sorgen, dass Datenverkehr, der als unautorisiert gelten müsste, trotzdem zugelassen wird. Welche der folgenden Möglichkeiten sollten Sie anwenden, um am effektivsten die Wirksamkeit des Angriffserkennungssystems zu testen und weitere Beiträge zu den Spezifikationen zu liefern?

a) Entwickeln Sie eine Serie von Szenarien, basierend auf vergangenen Ereignissen

b) Nutzern Sie einen Test, der böswilligen Datenverkehr generiert und neue Angriffsspezifikationen liefert

c) Verwenden Sie das Angriffserkennungssystem in Situationen von bekanntem böswilligem Datenverkehr

d) Nutzen Sie das Angriffserkennungssystem in Verbindung mit weiteren Angriffserkennungssystemen (IDS), falls möglich

B ist richtig, da diese Tests angewandt werden können, um neue Angriffsspezifikationen hinzuzufügen, die vorher als autorisiert gegolten hätten. A und C können hilfreich, aber dafür nicht so effektiv sein, um sicherzugehen, dass das System in Zukunft genauso gut funktioniert. D ist für den Systembetrieb, aber nicht zum Testen, richtig.

AS-5.6.1	(K2) Das Konzept der Malware-Scanner sowie deren Anwendung bei der Sicherung von Informationssystemen kennen
AS-5.6.2	(K3) Demonstrieren können, wie sich die Wirksamkeit bestehender Malware-Scanner testen lässt

Frage #30 (1 Punkt)

Welche der folgenden Möglichkeiten ist ein Hauptnachteil von Malware-Scannern (Schadsoftware-Scannern)?

a) Sie erkennen nur bestimmte Ebenen von Malware (Schadsoftware)

b) Sie können nur Malware erkennen, die dem Scanner bekannt ist

c) Sie neigen dazu, viel zu kompliziert zu sein, um sie überhaupt erst laufen zu lassen

d) Sie bieten keine Möglichkeit für Updates und Berichte

B ist richtig. Die Malware-Scanner können nur Malware (Schadsoftware) erkennen, die sie bereits kennen. A könnte richtig sein, abhängig des besonderen Schwerpunktes des Scanners, es handelt sich hierbei aber nicht um einen Hauptnachteil. C ist im Allgemeinen nicht richtig – die Scanner laufen normalweise sehr einfach. D ist nicht richtig, da die Scanner sehr wohl die Möglichkeit bieten sich zu aktualisieren und Berichte zu erstellen.

AS-5.7.1 (K2) Das Konzept der Datenmaskierung, Werkzeuge zur Datenmaskierung sowie deren Anwendung bei der Sicherung von Informationssystemen kennen

AS-5.7.2 (K3) Demonstrieren können, wie sich die Wirksamkeit von Datenmaskierungsansätzen testen lässt

Frage #31 (2 Punkte)

Um das Risiko während des Testens zu minimieren, müssen Sie die persönlichen Identifizierungsnummern aus einem Altsystem entfernen. Ein Teil Ihres Plans zur Datenverschleierung ist die Verifizierung der Effektivität zur Verdeckung der Daten. Welche der folgenden Möglichkeiten ist der effektivste Ansatz?

a) Manuelle Verifizierung innerhalb der Datenbank, um festzustellen, ob die durch Datenverschleierung veränderten Daten für die beabsichtigten Datensätze nicht mehr durch menschliche Interpretation zu verstehen sind

b) Eine Brute-Force-Attacke auf die maskierten Daten

c) Die sensiblen Daten mit zufälligen Daten von variierender Textlänge ersetzen

d) Die Entwicklerteams beauftragen, um ein Programm zu generieren, dass die Datenbank mit Angriffen belastet

B ist laut Lehrplan korrekt. Eine Brute-Force-Attacke oder Wörterbuchangriffe können verwendet werden, um zu überprüfen, ob persönliche Daten immer noch zugänglich sind. A ist nicht richtig, da dies aufgrund von Datenmenge und benötigter Zeit im Allgemeinen vermieden werden sollte. C ist nicht richtig, da das mehr eine Anonymisierungsaufgabe wäre. Außerdem könnte es sein, dass die Länge der Felder begrenzt ist, so dass das die Daten verändern würde. D ist nicht richtig, da wir nicht die Datenbank strapazieren wollen.

AS-5.8.1	(K2) Das Konzept der Sicherheitsschulung als Aktivität des Softwareentwicklungslebenszyklus und deren Notwendigkeit bei der Sicherung von Informationssystemen kennen
AS-5.8.2	(K3) Demonstrieren können, wie sich die Wirksamkeit von Sicherheitsschulungen testen lässt

Frage #32 (1 Punkt)

Was wird häufig als schwächstes Glied der Softwaresicherheit gesehen?

a) Das Fehlen eines konsistenten und umfangreichen Sicherheitsschulungsplans

b) Der benötigte Aktualisierungsaufwand von Dokumenten und Verfahren, um mit den aktuellen Sicherheitsgefahren mitzuhalten

c) Das menschliche Verhalten

d) Die konstante Weiterentwicklung von bösartigen Techniken

C ist richtig. Es ist das menschliche Verhalten, was als das schwächste Glied zählt. A, B und D sind Bedenken, aber C ist das schwächste Glied in der Sicherheitskette.

AS-6.1.1	(K2) Erläutern können, wie menschliches Verhalten zu Sicherheitsrisiken führen kann und inwieweit es die Wirksamkeit von Sicherheitstests beeinträchtigt
AS-6.3.1	(K2) Die Bedeutung des Sicherheitsbewusstseins für eine Organisation verstehen

Frage #33 (1 Punkt)

Welche der folgenden Möglichkeiten ist ein potenzielles Sicherheitsrisiko?

a) Ein Schaubild der Buchhaltungsabteilung einer Organisation auf einer Unternehmenswebsite veröffentlichen

b) Geburtstagswünsche für einen Mitarbeiter auf Facebook posten

c) Das Telefonbuch eines Unternehmens im zugehörigen Intranet posten

d) Die Berufserfahrung im LinkedIn-Profil angeben

A ist richtig. Diese Informationen könnten genutzt werden, um Genehmigungsketten für die Genehmigung von Rechnungen festzustellen, welche wiederum genutzt werden könnten, um falsche Rechnungen zu erstellen und zu genehmigen, sofern das Buchhaltungssystem gehackt werden würde. B ist falsch, da Geburtstage nicht in Informationen wie Passwörtern benutzt werden sollten (hoffen wir!). C ist falsch, da das Intranet eines Unternehmens hinter einer Firewall sein sollte, zusammen mit anderen geschützten Daten. D ist nicht richtig, da diese Informationen wahrscheinlich nicht hilfreich für einen Hacker sind.

AS-6.1.2	(K3) Wege für ein gegebenes Szenario identifizieren können, über die ein Angreifer wichtige Informationen über ein Ziel erlangen könnte, sowie Maßnahmen zum Schutz der Umgebung ergreifen können

Frage #34 (2 Punkte)

Sie sind dafür verantwortlich, die Finanzanwendung eines Unternehmens auf Sicherheit zu testen. Sie haben kürzlich eine E-Mail von einer Person erhalten, die behauptet, sich mit Shodan in das System gehackt und herausgefunden zu haben, dass eine veraltete und angreifbare Betriebssystemversion auf einem Ihrer Server läuft. Sie haben dies kontrolliert und festgestellt, dass der Hacker richtig liegt. Daraufhin haben Sie sichergestellt, dass der Server aktualisiert wird. Ihre vorausgehende Kontrolle konnte keine Hinweise liefern, wie der Hacker in Ihr System gelangen konnte. Sollten Sie Bedenken haben?

a) Nein, da dies ein „White-Hat“-Hacker ist und somit Ihrem Unternehmen nicht schaden will

b) Nein, Sie haben die Angriffsmöglichkeit behoben und das System ist nun sicher

c) Ja, das Sicherheitstesten ist nicht ausreichend und Sie müssen Ihre Tests erneut laufen lassen, um herauszufinden, was Sie übersehen haben

d) Ja, da der Hacker nicht mitgeteilt hat, wie er in das System gekommen ist, kann er sich immer noch Zugriff verschaffen und könnte die Schwachstelle das nächste Mal ausnutzen

D ist richtig und sollte Ihre größte Sorge in diesem Moment sein. A ist nicht richtig und könnte eine gefährliche Annahme sein. B ist nicht richtig, da der Hacker weiterhin Zutritt zu dem System hat. C könnte zwar wahr sein, aber die gleichen Tests noch einmal laufen zu lassen, würde das Problem nicht lösen.

AS-6.1.3	(K2) Die allgemeinen Motive und Quellen für die Durchführung von Angriffen auf Computersysteme erläutern können
AS-6.2.1	(K2) Erläutern können, wie Sicherheitsvorkehrungen durch Social Engineering umgangen werden können

Frage #35 (1 Punkt)

Warum ist ein Angriff aus dem Inneren einer Organisation besonders besorgniserregend?

a) Der Angreifer ist wahrscheinlich durch Neugierde angetrieben und wird unnachgiebig sein

b) Der Angreifer ist wahrscheinlich während der Arbeit gelangweilt und wird mit dem „Hacken zur Unterhaltung“ weitermachen

c) Der Angreifer ist schon innerhalb der Firewall und gilt als autorisierter Nutzer des Systems

d) Der Angreifer wird sehr wahrscheinlich einen DOS-Angriff starten, welcher die Server zerstören wird

C ist richtig. Die größte Gefahr hierbei ist, dass der externe Schutz wirkungslos ist, da der Angreifer schon innerhalb des Systems ist. A und B sind wahrscheinlicher bei externen Hackern. D ist nicht die wahrscheinlichste Attacke – im Allgemeinen sind interne Nutzer mehr auf der Suche nach Informationen, die sie verkaufen oder die genutzt werden können, um das Unternehmen bloß zu stellen.

AS-6.1.4	(K4) Ein Angriffsszenario (Angriff durchgeführt und entdeckt) analysieren sowie mögliche Quellen und Motive für den Angriff ermitteln können

Frage #36 (3 Punkte)

Sie arbeiten in einer Organisation, in der der Zugriff auf die Server für die Systemadministration stark eingeschränkt ist. Nur drei eingeweihte Festangestellte kennen das „root“-Passwort. Kürzlich haben sich jedoch mehrere seltsame Vorfälle ereignet. Es wurde ein unbekanntes Programm namens „IchKenneDeinenGeburtstag“ gefunden, was Geburtstagsgrüße an Mitarbeiter verschickt. Die Geburtstage sind richtig und die Grüße wurden alle jeweils unterzeichnet mit „Von Ihrem liebsten Server“. Das Programm wurde entfernt, jedoch konnte keiner herausfinden, wo es herkam. Ein zweites Problem tauchte auf, als die unternehmensweite Telefonliste gehackt wurde und alle Telefonnummern zu 867-5309 geändert wurden. Die richtige Liste wurde wiederhergestellt, und es konnte wieder nicht herausgefunden werden, wie das gemacht wurde, obwohl eine neue „root“-Datei erstellt wurde. Sie haben gerade einen Anruf des leitenden Systemadministrators bekommen, der Ihnen mitteilte, dass das „root“-Passwort geändert wurde. Es wurde festgestellt, dass das Passwort der Name des Hundes des leitenden Systemadministrators war.

Weitere Nachforschungen haben ergeben, dass das Problem auftrat, kurz nachdem eine Reihe von virusbefallenen E-Mails bemerkt wurde. Als die erste von ihnen gefunden wurde, wurden sofort Sicherheitswachen aufgestellt, um die Verbreitung des Virus zu stoppen, aber nun wundern Sie sich, ob jemand mithilfe von Code, der durch den Virus in das System gelangt ist, in das System eingreifen konnte.

Was sollte Ihr nächster Nachforschungsschritt sein?

a) Nachsehen, ob auf die Geburtstagsinformationen von HR von außen zugegriffen wurde und, wenn ja, die IP-Adresse nachverfolgen

b) Verifizieren, ob der Name des Hundes des leitenden Systemadministrators auf sozialen Medien gepostet wurde

c) Die verdächtige E-Mail untersuchen und versuchen diese IP-Adresse zurückzuverfolgen

d) Die Personalakten der anderen zwei Systemadministratoren untersuchen, um zu sehen, ob es irgendwelche Anzeichen für Unzufriedenheit bei ihnen gibt

C ist richtig. Das ist der beste Anfangspunkt, denn es scheint, als könnte dies der Ursprung des Problems sein. Falls C nichts Zufriedenstellendes ergibt, dann sind A und D die nächsten wahrscheinlichen Möglichkeiten, die es zu verfolgen gilt, da es möglich ist, dass es sich um eine interne Attacke handelt (D) oder dass die Attacken unabhängig voneinander waren. Die Geburtstagsinformationen (A) könnten daher Hinweise geben, wer hierfür in Frage käme. B könnte zwar in dieser Weise angegangen werden, aber es wäre einfacher, den Systemadministratoren zu fragen, wer den Namen seines Hundes kennen könnte.

AS-6.3.2	(K3) Ausgehend von bestimmten Testergebnissen, entsprechende Maßnahmen zur Erhöhung des Sicherheitsbewusstseins einleiten können

Frage #37 (2 Punkte)

Während des Testens eines Upgrades finden Sie heraus, dass es möglich ist, eine „Man-In-The-Middle“-Attacke zu starten, die dann den zu zahlenden Betrag der Kunden in Ihrer e-Commerce-Seite verändern kann. Ihre Tester haben es erfolgreich geschafft, den Betrag so zu setzen, dass alle Kunden einen Rabatt von 10% kriegen. Was sollten Sie nun als erstes tun?

a) Den Testern sollte abgeraten werden, solche Arten von Attacken zu testen, denn sie sind in der Produktionsumgebung unrealistisch

b) Sofort das Management informieren, dass die Attacke als Teil eines Tests kreiert wurde, für den Fall, dass sie bemerkt wird

c) Mit den Entwicklern arbeiten, um Kontrollen wie SSL-Strip durchzuführen, um sicher zu gehen, dass die Zertifikate gültig sind und nicht selbstsigniert

d) Die Produktionsumgebung überprüfen, um zu sehen, ob der angreifbare Code auch in der Produktion ist

D ist richtig. Erste Priorität ist es, zu sehen, ob die Angriffsstelle auch im Produktionscode ist und dann das Problem sofort zu beheben. C sollte der nächste Schritt sein, um sicher zu gehen, dass die Entwickler richtig programmieren und alle zur Verfügung stehenden Mittel nutzen, um auf diese Art Fehler zu testen. A ist falsch, da das genau das ist, was Sicherheitstester machen sollen. B ist falsch, da die Erlaubnis des Managements immer schon vor den Tests eingeholt werden sollte und nicht erst danach.

AS-7.1.1	(K2) Die Gründe verstehen, warum Sicherheitserwartungen und Abnahmekriterien entsprechend der Veränderung des Umfangs und der Ziele eines Projekts angepasst werden müssen

Frage #38 (1 Punkt)

Warum ist es wichtig, Sicherheitsrisikoerwartungen regelmäßig neu einzuschätzen?

a) Stakeholder müssen zu jedem Zeitpunkt über alle Sicherheitsrisiken informiert sein

b) Stakeholder treffen Geschäftsentscheidungen auf Basis der entsprechenden Sicherheitsrisikolevels

c) Nutzer müssen einen auf einem Handbuch basierenden, vorbeugenden Plan entwickeln

d) Sowohl die Erwartungen der Nutzer als auch die der Stakeholder zum Thema „Sicherheit“ sollten nicht verändert werden

B ist richtig. Stakeholder müssen oft Geschäftsentscheidungen bezüglich des akzeptierten Sicherheitsrisikolevels und notwendiger, vorbeugender Maßnahmen treffen. A ist nicht richtig, da nicht jeder alles wissen muss. C ist nicht richtig, da ein auf einem Handbuch basierender Risikovermeidungsplan unpraktikabel ist und Nutzer diesen wahrscheinlich eh nicht implementieren würden. D ist nicht richtig, da Erwartungen sich sehr wohl ändern sollten.

AS-7.2.1	(K2) Die Wichtigkeit verstehen, Ergebnisse von Sicherheitstests vertraulich und sicher zu halten
AS-7.2.2	(K2) Verstehen, warum die richtigen Steuer- und Datenerfassungsmechanismen geschaffen werden müssen, damit die Ausgangsdaten für die Statusberichte von Sicherheitstests zeitnah und präzise bereitgestellt werden können (z.B. ein Sicherheitstest-Dashboard)

Frage #39 (1 Punkt)

Welche der folgenden Möglichkeiten ist ein wichtiger Aspekt bei Sicherheitstestergebnissen?

a) Sie werden für Nutzer und Stakeholder zugreifbar veröffentlicht, um diesen ein besseres Verständnis des Risikos zu geben

b) Sie sollten mit Entwicklern innerhalb des Unternehmens geteilt werden, um das Risiko für zukünftige Entwicklungsprojekte zu mindern

c) Je weniger Leute es wissen, desto besser

d) Testergebnisse sollten immer entlang ihrer Kritikalität klassifiziert werden

C ist richtig. Die Ergebnisse eines Sicherheitstests sollten vertraulich gehandhabt werden und der Zugriff auf die Ergebnisse sollte streng kontrolliert sein. Hintergrund hierzu ist, dass die Ergebnisse eines solchen Tests häufig Schwächen in dem aktuell zu testenden System aufdecken. Die hier gefundenen Probleme sind häufig dieselben Probleme, wie im Produktionssystem. A ist nicht richtig, da der Zugang zu den Ergebnissen streng kontrolliert werden muss. B ist nicht richtig, da nur einzelne Teile des Berichts (nur die, zur Verbesserung der Programmierung) für die Entwickler erreichbar gemacht werden sollten. Gleichermaßen sollten einzelne Teile für die Mitarbeiter aus dem Infrastrukturbereich verfügbar sein, um Probleme, die in der Infrastruktur gefunden werden könnten, zu verbessern. D ist wahr, ist aber nicht der wichtigste Aspekt.

AS-7.2.3 (K4) Einen gegebenen Zwischenbericht der Sicherheitstests analysieren können, um den Grad an Genauigkeit, Verständlichkeit und Zweckmäßigkeit für die Stakeholder erfassen zu können

Frage #40 (3 Punkte)

Sie finalisieren Ihren Sicherheitsteststatusreport für ein Projekt, das bereit ist, in der Produktion gestartet zu werden. Aufgrund der Beschaffenheit des Systems gibt es einen hohen Risikograd. Daher wollen Sie einen besonderen Fokus auf das Thema Risiko legen. Welche Möglichkeit ist, basierend auf diesen Kenntnissen, die beste, um das Risiko deutlich zu machen?

a) Eine anschauliche Risikobewertung, die in der Zusammenfassung enthalten ist

b) Das allgemeine Risiko im letzten Abschnitt des Reports

c) Risikoauswirkungen, die in der Zusammenfassung und später, anhand von speziellen Angriffsmöglichkeiten, detaillierter beschrieben werden

d) Risikoauswirkungen sind kein Teil der Zusammenfassung eines Reports

C ist richtig. Die Risikoauswirkungen sollten in der Zusammenfassung beschrieben und später im Report detailliert werden, sofern genaue Angriffsmöglichkeiten aufgeführt werden. A ist nicht richtig, da die Details nicht in der Zusammenfassung sein sollten. B ist nicht richtig, da diese Informationen nicht nur am Ende des Reports aufgeführt werden sollten. D ist nicht richtig, da es ein wichtiger Teil des Reports ist.

AS-8.1.1 (K2) Die Funktion statischer und dynamischer Analysewerkzeuge bei Sicherheitstests erläutern können

Frage #41 (1 Punkt)

In welcher Weise unterscheiden sich dynamische Sicherheitsanalysewerkzeuge von allgemeinen, dynamischen Analysewerkzeugen?

a) Die Sicherheitswerkzeuge sondieren eher das System statt die zu testende Anwendung

b) Die Sicherheitswerkzeuge funktionieren im dynamischen oder statischen Modus gleich

c) Die Sicherheitswerkzeuge sind besser geeignet, Probleme wie z.B. Memory-Leaks (Speicherlöcher) zu finden

d) Die Sicherheitswerkzeuge müssen genau auf die Sprache zugeschnitten sein, in der die Anwendung implementiert wurde

A ist richtig. B ist nicht richtig, da es beides, sowohl statische als auch dynamische Sicherheitsanalysewerkzeuge, gibt. C ist nicht richtig, da Memory Leaks durch allgemeine dynamische Analysewerkzeuge, und nicht durch die sicherheitsspezifischen Werkzeuge, gefunden werden. D ist nicht richtig, da das auf alle statischen Analysewerkzeuge zutrifft.

AS-8.2.1	(K4) Sicherheitstesterfordernisse, denen mit einem oder mehreren Werkzeugen Rechnung getragen wird, analysieren und dokumentieren können

Frage #42 (3 Punkte)

Sie wurden beauftragt, die Firewall einer Organisation zu testen. Sie haben schon den Implementierungsplan und die zugehörigen Schritte überprüft. Sie haben verifiziert, dass die Konfiguration so eingerichtet wurde, wie der Lieferant der Firewall es vorschreibt, sowie einen Port-Scan vorgenommen. Ihre Organisation macht sich besondere Gedanken um eine Dienstblockade (DOS-Attacke), da es bereits eine gab, als die alte Firewall noch in Betrieb war. Welche Art von Test sollten Sie durchführen, um unerwartetes Verhalten, das mit einer DOS-Attacke ausgenutzt werden könnte, zu erkennen?

a) Sie sollten Tests erstellen, die falsch strukturierte Netzwerkpakete oder Fuzz-Daten senden und dann sehen, ob diese von der Firewall erkannt und abgelehnt werden

b) Sie sollten automatisierte Tests implementieren, als Stresstest für die Server und, um die Ausfallsicherung zu testen

c) Sie sollten die Verschlüsselungs- und Entschlüsselungsalgorithmen testen, um festzustellen, ob sie schnell genug sind, um mit der Belastung einer DOS-Attacke umzugehen

d) Sie sollten die Härtung von Softwarekomponenten testen, um sicher zu gehen, dass die Angriffsfläche so klein wie möglich ist

A ist richtig, da dies beides Techniken sind, die genutzt werden, um Firewalls zu testen. B und C sind nicht richtig, da es eher das Ziel ist, die Attacke zu verhindern, als durch die Firewall hindurchzulassen. D ist nicht richtig, da Softwarekomponentenhärtung zwar den individuellen Softwarekomponenten hilft, aber nicht der Firewall und ihrer Implementierung.

AS-8.2.2	(K2) Die Probleme von Open-Source-Werkzeugen verstehen
AS-8.2.3	(K2) Beurteilen können, ob ein Anbieter in der Lage ist, Werkzeuge häufig zu aktualisieren oder im Hinblick auf Sicherheitsgefährdungen auf dem neuesten Stand zu halten

Frage #43 (1 Punkt)

Welche der folgenden Möglichkeiten ist eine wichtige Überlegung für die Instandhaltung eines Werkzeugs, das unter der GNU General Public License verwendet werden soll?

a) Verlässlichkeit des Lieferanten und dessen Fähigkeit, Unterstützung zu bieten

b) Häufigkeit und Verfügbarkeit von Aktualisierungen des Lieferanten

c) Technische Fertigkeiten Ihres Teams, um das Werkzeug in Ihrer Umgebung zu unterhalten und für diese anzupassen

d) Lizenzkosten und unterstützende Vertragskosten

C ist richtig. Die GNU Lizenz ist kostenlos und entspringt einer Open-Source-Gemeinschaft, es gibt also nicht zwangsläufig einen direkten Lieferanten im eigentlichen Sinne. A und B sind daher falsch, da es zwangsläufig keinen Lieferanten gibt. D ist falsch, denn das Werkzeug ist kostenlos, auch wenn Sie Entwicklungskosten aufgrund der Anpassung an Ihre Bedürfnisse haben könnten.

AS-9.1.1	(K2) Die Vorteile der Verwendung von Sicherheitsteststandards kennen und wissen, wo diese zu finden sind
AS-9.3.1	(K2) Informationsquellen für Branchentrends in der Informationssicherheit kennen

Frage #44 (1 Punkt)

Welche der folgenden Möglichkeiten ist ein Vorteil der Verwendung von Sicherheitsstandards?

a) Sie sind konsistent und einfach zu befolgen, da sie separat und unabhängig von Projektzielen und -plänen sind

b) Sie liefern Bausteine für zukünftiges Testen, wodurch es möglich ist, nicht jedes Mal von ganz vorne beginnen zu müssen

c) Sie beschreiben eine effektive Offensive, mit der Gefahren beseitigt werden, bevor sie ins System gelangen

d) Sie erlauben Spielraum in Sicherheitspraktiken, da Gefahren sich immer dynamisch verändern

B ist richtig. A ist nicht richtig, da Sicherheitsstandards in Projektzielen und -plänen erwähnt sein können. C ist nicht richtig, da sie von Natur aus defensiv sind. D ist nicht richtig, da sie bestimmte Standards definieren, die in der Praxis helfen. Diese Standards sollten auf Veränderungen von Gefahren reagieren.

AS-9.1.2	(K2) Den Unterschied in der Anwendbarkeit von Standards für regulatorische und vertragliche Situationen verstehen
AS-9.2.1	(K2) Den Unterschied zwischen obligatorischen (normativen) und optionalen (informativen) Klauseln in Standards kennen

Frage #45 (1 Punkt)

Welche der folgenden Möglichkeiten ist ein Vorteil von vertraglich auferlegten Sicherheitsstandards?

a) Sie bieten jeder Partei eine legale Ausstiegsmöglichkeit, wenn ein unvorhergesehenes Sicherheitsproblem das Produkt nachteilig beeinflusst

b) Sie bieten beiden Seiten eine gute Grundlange für Verhandlungen

c) Sie sind ein geeigneter Weg, öffentliche Vereinbarungen zwischen zwei Parteien zu treffen

d) Die Verträge ändern sich automatisch, wenn sich die Standards ändern, selbst wenn die Verträge bereits geschlossen sind.

B ist richtig. Durch das Definieren von Sicherheitsstandards kann jede Seite ermitteln, was gefordert wird und diese Anforderungen weiter spezifizieren. A ist nicht richtig, da es dann schon zu spät ist. C ist nicht richtig, da die Sicherheitsvereinbarungen meistens geheim gehalten werden. D ist nicht richtig, da Verträge sich normalerweise nicht auf diese Weise ändern.