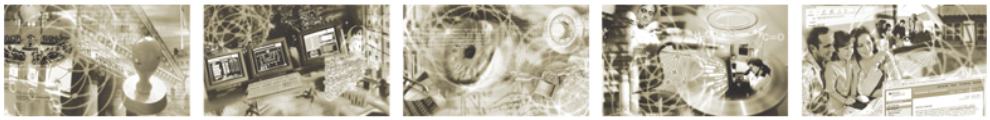
Bundesamt
für Sicherheit in der
Informationstechnik



Ein Praxis-Leitfaden für IS-Webchecks

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: it-pentest@bsi.bund.de
Internet: https://www.bsi.bund.de

Stand: Version 1.0 (November 2016)

Inhaltsverzeichnis

1 Einleitung 4
1.1 Adressatenkreis 4
1.2 Zielsetzung 4
1.3 Begriffsbestimmung IS-Webcheck 5
1.4 Abgrenzungen 7
1.4.1 Grenzen des Leitfadens 7
1.4.2 Abgrenzungen für IS-Webchecks 7
1.4.3 Abgrenzungen zu anderen IT-Sicherheitstests 8
2 Organisatorische Voraussetzungen für einen IS-Webcheck 10
2.1 Anforderung an die Institution 10
2.1.1 Motivation für einen IS-Webcheck 10
2.1.2 Rahmenbedingungen für IT-Sicherheitstests 10
2.2 Anforderungen an einen Prüfer 12
2.2.1 Fachliche Anforderungen 12
2.2.2 Weitere Fähigkeiten 12
2.2.3 Technische Qualifikation / Zertifikate 13
2.2.4 Verwendete Tools 14
2.3 Weitere Rahmenbedingungen 14
3 Fachliche Voraussetzungen für einen IS-Webcheck 17
3.1 Festlegung des Prüfobjekts zwischen Prüfer und Institution 17
3.2 Festlegung des Prüfumfangs 17
3.3 Dokumentation 19
3.4 Verantwortlichkeiten 20
4 Ablauf eines IS-Webchecks 22
4.1 Einarbeitung der Prüfer 22
4.2 Test des Prüfobjekts 22
4.3 Bericht 28
5 Anhang: 30
5.1 Checklisten 30
5.1.1 Hilfestellung für die Beauftragung von Prüfern 30
5.1.2 Mindestanforderungen an einen IS-Webcheck 31
5.2 Ablaufplan 34
6 Glossar 35
7 Referenzen 39

1 Einleitung

Es ist inzwischen den meisten IT-Anwendern bewusst, dass Angriffe auf IT-Systeme tatsächlich stattfinden und auch „vermeintlich“ weniger attraktive Ziele in den Fokus von Angreifern geraten. Daher sollten besonders IT-Verantwortliche, die mit vernetzten IT-Systemen arbeiten, neben den selbstverständlich gewordenen Absicherungsmaßnahmen auch IT-Sicherheitstests durchführen, die darauf spezialisiert sind, Angriffsmöglichkeiten zu entdecken.

Im Folgenden wird der IT-Sicherheits-Webcheck oder kurz IS-Webcheck als eine spezielle Variante des IS-Penetrationstests [7] beschrieben, bei dem die Absicherung von Webanwendungen überprüft wird. Das vorliegende Dokument soll als Leitfaden für die Beauftragung von IS-Webchecks dienen und die Rahmenbedingungen bei der Durchführung erläutern.

Im ersten Kapitel wird eine Möglichkeit, einen IS-Webcheck zu gestalten, beschrieben. Der Fokus liegt auf einer Zeit- und Kosten sparenden Vorgehensweise, die aus den praktischen Erfahrungen des BSI entwickelt wurde. Es werden daher aus den unterschiedlichen Möglichkeiten einen IS-Webcheck zu gestalten, klare Empfehlungen für jeweils die Variante gegeben, die sich als die Effizienteste erwiesen hat. Auf diese Empfehlungen bauen alle im Dokument beschriebenen Rahmenbedingungen und Abläufe auf.

1.1 Adressatenkreis

Das vorliegende Dokument wendet sich vorrangig an alle Verantwortlichen in Unternehmen und Behörden (im Folgenden Institutionen genannt), die über die gängigen Schutzmaßnahmen ihrer IT-Systeme und Daten hinaus IS-Webchecks als Testverfahren einzusetzen beabsichtigen, um Angriffsmöglichkeiten auf ihre Daten zu identifizieren.

Auch Anbieter von IS-Webchecks (im Folgenden Prüfer genannt) seien angeregt, das Dokument zu lesen und ihre eigene Vorgehensweise zu hinterfragen.

1.2 Zielsetzung

Der Praxis-Leitfaden soll Institutionen bei der Beauftragung von IS-Webchecks unterstützen, in dem er die zu erwartende Vorgehensweise beschreibt und auf Aspekte hinweist, auf die bei einem IS-Webcheck geachtet werden sollte.

IT-Sicherheitsbeauftragten und weiteren Verantwortlichen für die Informationssicherheit soll dieser Leitfaden insbesondere dazu dienen, sich einen Überblick über das Thema IS-Webcheck zu verschaffen und sich mit dem Ablauf vertraut zu machen.

Prüfern werden konkrete Empfehlungen für den Ablauf eines IS-Webchecks angeboten. Diese sind insbesondere in Kapitel 4 „Ablauf eines IS-Webcheck“ zu finden.

Die Inhalte basieren auf der Praxiserfahrung der BSI-Prüfer. Es wurde eine allgemein praktizierte Vorgehensweise für IS-Webchecks beschrieben. Stellen im Text, bei denen eine spezielle Vorgehensweise aus der BSI-Praxis empfohlen wird, werden wie folgt gekennzeichnet:

Das BSI empfiehlt...

1.3 Begriffsbestimmung IS-Webcheck

Das BSI versteht unter einem IS-Webcheck ein erprobtes und geeignetes Vorgehen, um das aktuelle Sicherheitsniveau einer Webanwendung festzustellen. Der IS-Webcheck dient dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf die Webanwendung einzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten bzw. die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen. Für sicherheitskritische Webanwendungen sollten regelmäßig IS-Webchecks erfolgen.

Eine Webanwendung ist nach der hier verwendeten Definition Teil eines Webauftritts. Dieser besteht aus (ggf. mehreren) Webanwendungen, die auf einem Webserver laufen und mit anderen Anwendungen oder Datenbanken kommunizieren und über eine Netzwerkschnittstelle wie beispielsweise das Internet für Anwender erreichbar ist. Der Webauftritt ist darüber hinaus meistens durch ein Sicherheitsgateway geschützt (Siehe auch Abb. 1).

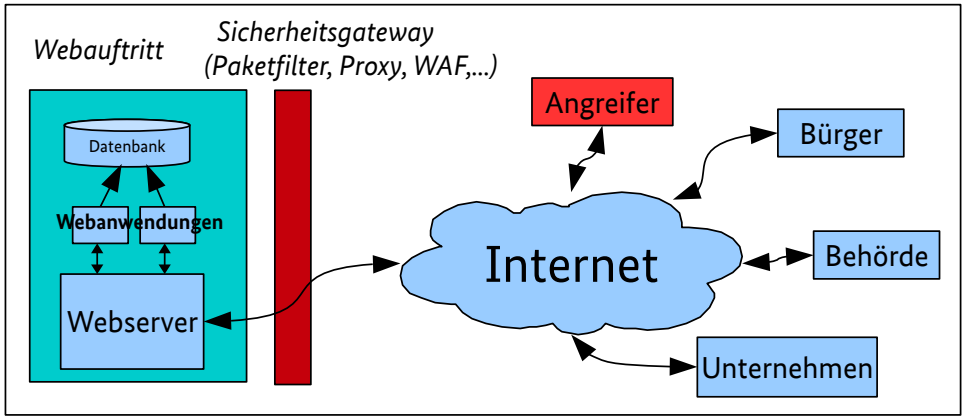


Abbildung 1 Webauftritt

Das BSI empfiehlt in verschiedenen Veröffentlichungen ([8],[9],[10]) bei der Absicherung eines Webauftritts jede einzelne Komponente separat abzusichern und sich nicht auf die alleinige Absicherung durch ein Sicherheitsgateway zu verlassen.

Auch wenn durch spezielle Komponenten des Sicherheitsgateways der Schutz eines Webauftritts deutlich erhöht werden kann, können Angreifer unter Umständen weiterhin in die Systeme eindringen, wenn diese nicht separat abgesichert sind. Bei einer eventuellen Fehlkonfiguration oder einer ausgenutzten Schwachstelle im Sicherheitsgateway, kann ein Angreifer trotzdem ein potenziell verwundbares System hinter dem Schutzwall finden und angreifen, wenn die Webanwendung oder die beteiligten Anwendungen und Datenbanken nicht selbst ausreichend abgesichert sind.

Es ist weiterhin zu beachten, dass oftmals die Sicherheitsgateways eine Vielzahl von Systemen absichern und damit sehr generisch gegen Angriffe aufgestellt werden. Hierbei kann die Absicherung, die für die eine Anwendung notwendig ist, für eine andere Anwendung hinderlich sein. In einem solchen Fall werden oftmals kurzfristig Regeln gelockert, ohne zu prüfen, ob hierdurch eine andere Anwendung angreifbar wird.

Darüber hinaus werden innerhalb eines Sicherheitsgateways bekannte Angriffsmuster abgewehrt. Findige Angreifer entwickeln jedoch täglich neue Methoden um Angriffe durchzuführen. Eine parameterbezogene Eingabevalidierung innerhalb der Webanwendung kann hier viele Schwächen von vornherein ausschließen.

Da die Webanwendung den Teil des Webauftritts darstellt, mit dem der Anwender kommuniziert, wird bei einem IS-Webcheck hauptsächlich die Absicherung der Webanwendung getestet. Die Durchführung eines IS-Webchecks erfolgt dabei grundsätzlich über das Netz, über das der Webauftritt erreichbar ist. In den meisten Fällen ist dies das Internet. Die weiteren Komponenten des Webauftritts können viel effektiver durch einen 'vor Ort' stattfindenden IS-Penetrationstest separat geprüft werden.

Damit die Webanwendungen für den IS-Webcheck ohne Filterung durch ein Sicherheitsgateway erreichbar ist, muss für die Prüfer ein direkter Weg freigeschaltet werden. Ist dies nicht möglich, kann nur eine diffuse Momentaufnahme des Zusammenspiels zwischen Sicherheitsgateway und Webauftritt gemacht werden, was die klare Umsetzung von Empfehlungen für die Absicherung der einzelnen Komponenten für den Auftraggeber nach Abschluss der Tests erschwert.

IS-Webchecks können in unterschiedlicher Tiefe durchgeführt werden. Zu vermeiden sind destruktive Tests, d. h. Tests, bei denen die Zielsysteme zu Schaden kommen könnten, wie es beispielsweise durch das Ausnutzen der Schwachstellen geschehen kann. Da bei einem IS-Webcheck jedoch, anders als bei einem IS-Penetrationstest, über nur eine Schnittstelle verschiedene Systeme angesprochen werden, können manche Schwachstellen nur durch das Ausnutzen gefunden werden. Nur so kann nachgewiesen werden, dass beispielsweise die Datenbank oder andere Anwendungen hinter der Webanwendung vom Anwender direkt angesprochen werden können.

Auch eine mangelnde Eingabevalidierung kann bei einem IS-Webcheck in den meisten Fällen nur durch Ausnutzen der Schwachstelle nachgewiesen werden.

> Das BSI empfiehlt allerdings, dass nur gut getestete Exploits zum Einsatz kommen und dass soweit es möglich ist, die Schwachstellen ohne den Einsatz von Exploits nachgewiesen werden.

Ebenso wie IS-Penetrationstests können IS-Webchecks als Whitebox- oder Blackbox-Test ausgelegt werden. Bei einem Blackbox-Test stehen den Prüfern lediglich die Adressinformationen des Zieles zur Verfügung, weitere Informationen werden nicht mitgeteilt. Bei der Vorgehensweise "Blackbox-Test" soll der Angriff eines typischen Außentäters simuliert werden, der nur unvollständige Kenntnisse über das Zielsystem hat. Dagegen verfügen die Prüfer bei einem Whitebox-Test über umfangreiche Informationen über die zu testenden Systeme. Dazu gehören beispielsweise Informationen über das eingesetzte Content-Managementsystem (CMS), eingesetzte Betriebssysteme, Datenbanken und weitere Hilfsanwendungen. Diese Angaben werden den Prüfern vor der Prüfung vom Auftraggeber mitgeteilt.

Das BSI empfiehlt, grundsätzlich Whitebox-Tests durchzuführen, da bei einem Blackbox-Test aufgrund nicht vorliegender Informationen Schwachstellen übersehen werden können. Auch besteht bei einem Blackbox-Test ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden zu verursachen. Zusätzlich ist der Aufwand bei einem Blackbox-Test wesentlich größer als bei einem Whitebox-Test.

Da es im Bereich der Webanwendungen eine Vielzahl von unterschiedlichen Möglichkeiten gibt, Inhalte darzustellen, existieren eine Vielzahl von Angriffsmöglichkeiten, die sich täglich weiter vermehren. Darüber hinaus sind die meisten Webanwendungen sehr umfangreich. Hierdurch ist es nicht immer möglich, in einer vertretbaren Zeit manuelle Tests durchzuführen, so dass bei einem IS-Webcheck häufig automatisierte Tools zum Einsatz kommen. Dennoch gehört aus Sicht des BSI zu einem IS-Webcheck, dass stichprobenartig weitere manuelle Tests durchgeführt und die mit den automatisierten Methoden gefundenen Schwachstellen manuell verifiziert werden.

1.4 Abgrenzungen

1.4.1 Grenzen des Leitfadens

Das Dokument beinhaltet keine Checkliste für Institutionen, mit der Anbieter von IS-Webchecks bei der Arbeit überprüft werden können. Ebenso wenig enthält er eine Checkliste für Prüfer, die abgearbeitet werden kann.

Auch Angreifer arbeiten nicht nach Checklisten, sondern schauen sich das Angriffsziel an und richten ihre Angriffe gezielt auf die vorgefundenen IT-Systeme und deren mögliche Schwachstellen. Ein guter IS-Webcheck zeichnet sich dadurch aus, dass er flexibel auf jede Gegebenheit neu angepasst wird.

Die im Anhang beigefügten Checklisten sollen bei der Beauftragung von IS-Webchecks unterstützen und dabei helfen, die organisatorischen und fachlichen Rahmenbedingungen einzuhalten, die bei einem IS-Webcheck erfüllt werden müssen. Darüber hinaus sind in den Checklisten die wiederkehrenden Elemente eines IS-Webcheck enthalten.

1.4.2 Abgrenzungen für IS-Webchecks

Ein IS-Webcheck ersetzt keine Qualitätssicherung von neuen oder geänderten Webanwendung. Die erforderliche Qualitätssicherung muss in jeder Institution in den Lebenszyklus der eingesetzten Webanwendung integriert sein.

Die Prüfer müssen zu jeder Zeit unabhängig von dem Prüfobjekt bleiben, damit sie, ähnlich wie Angreifer, neue Ideen aus einem unbeteiligten Blickwinkel heraus entwickeln können. Das bedeutet beispielsweise, dass ein IS-Webcheck nicht durch die hauseigenen IT-Fachkräfte durchgeführt werden sollte.

Die Unabhängigkeit und Flexibilität gehen auch verloren, wenn die Prüfer zyklisch überprüfen, ob die beim letzten Mal von ihnen gefundenen Schwachstellen beseitigt worden sind. Diese Überprüfungen müssen unter Einbeziehung des IT-Sicherheitsmanagements durch die interne Qualitätssicherung oder das interne IT-Personal erfolgen. Hierbei sollten reproduzierbare Testverfahren eingesetzten werden, welche nach jeder Änderung eines IT-Systems oder einer Anwendung erneut prüfen, ob die erforderliche Qualität und Sicherheit erreicht ist. Auch viele der durch die Prüfer gefundenen Schwachstellen können für alle zukünftigen internen Prüfungen in das Testrepertoire der Qualitätssicherung aufgenommen werden.

Die meisten IS-Webchecks sind sowohl zeitlich als auch von ihrem Umfang her begrenzt und beziehen sich nur auf die zu erwartenden Hauptangriffsziele der Webanwendung. Daneben können aber auch weitere Schwachstellen in anderen benachbarten IT-Systemen vorhanden sein.

Der IS-Webcheck, wie das BSI ihn definiert, beinhaltet weiterhin keinerlei Elemente des Social Engineering. Reale Angriffe würden höchstwahrscheinlich über Elemente des Social Engineering gestartet werden oder solche beinhalten. Bei Social Engineering Angriffen werden über die Gutgläubigkeit der Mitarbeiter, aber auch über Informationen, die im Internet

(beispielsweise Social Media oder Foren) frei verfügbar sind, Kenntnisse über die Strukturen einer Institution und auch über deren IT-Systeme zusammengetragen, um mit weiteren Angriffen gezielt darauf aufbauen zu können. Es wird empfohlen, dass Institutionen ihre Mitarbeiter in einem hohen Maß für solche Angriffsmethoden sensibilisieren. Die Simulation eines Social Engineering-Angriffs kann zwar auf der einen Seite die Aufmerksamkeit für solche Methoden stark verbessern, die Erfahrung zeigt aber, dass sich einzelne Mitarbeiter durch nachgestellte Social Engineering Aktionen bloßgestellt sehen, wenn diese bei ihnen erfolgreich waren. Um dies zu vermeiden, sollten solche Tests nur unter genau definierten Rahmenbedingungen unter Einbeziehung der Personalvertretung mit darauf trainierten Spezialisten durchgeführt werden.

1.4.3 Abgrenzungen zu anderen IT-Sicherheitstests

Es gibt verschiedene Methoden, die Sicherheit von Netzen, IT-Systemen und IT-Anwendungen zu überprüfen. Im folgenden Abschnitt werden die Unterschiede von IS-Webchecks zu den gängigen Methoden beschrieben.

IS-Revisionen

Die Hauptaufgabe der IS-Revision ist es, das Management, das IS-Management-Team und insbesondere den IT-Sicherheitsbeauftragten bei der Umsetzung und Optimierung der Informationssicherheit zu unterstützen und zu begleiten. Die Prüftätigkeit zielt darauf ab, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und der Sicherheitsprozesse zu optimieren.

Während die IS-Revision basierend auf IT-Grundschutz überprüfen soll, ob die vorher festgelegten Sicherheitsmaßnahmen wie vereinbart umgesetzt sind, geht der IS-Webcheck einen Schritt weiter. Es wird hierbei gezielt nach Wegen gesucht, die eingesetzten Sicherheitsmaßnahmen zu umgehen.

Code-Review

Bei einem Code-Review wird der Quellcode von Software systematisch auf Schwachstellen und Fehler untersucht. Der Code-Review ist ein Teilgebiet der Qualitätssicherung. Er kann aber auch gezielt eingesetzt werden, um gängige Sicherheitslücken zu finden. Hierzu wird der Quellcode beispielsweise gezielt nach zu gering ausgelegten Speicherbereichen oder nicht abgefangenen Fehlern untersucht. Bei einem IS-Webcheck wird im laufenden Betrieb gezielt unerwartetes Verhalten provoziert und anhand des Verhaltens der IT-Anwendung auf Schwachstellen geschlossen.

IS-Penetrationstest

Bei IS-Penetrationstests werden vorrangig Schnittstellen untersucht, über die potenzielle Angreifer in die untersuchten IT-Systeme eindringen könnten. Hierbei werden Konfigurationsfehler sowie noch nicht behobene Schwachstellen identifiziert.

Ein IS-Webcheck ist ein Spezialfall eines IS-Penetrationstests. Mit einem IS-Webcheck wird der Sicherheitsstand einer Internetpräsenz einer Institution geprüft. Hierbei werden die

Webanwendungen größtenteils durch den Einsatz automatisierter Methoden über das Internet geprüft.

Wenn ein vollständiger Sicherheitsstatus für einen Webauftritt erwünscht ist, wird empfohlen, einen IS-Penetrationstest zusätzlich zu dem IS-Webcheck durchzuführen.

2 Organisatorische Voraussetzungen für einen IS-Webcheck

Bevor ein IS-Webcheck durchgeführt werden kann, sollten verschiedene organisatorische Voraussetzungen erfüllt sein. In den folgenden Unterkapiteln wird beschrieben, welche Erwartungen an die beteiligten Gruppen vor einem IS-Webcheck gestellt werden.

2.1 Anforderung an die Institution

Es ist selbstverständlich, dass ein Prüfer gewisse Anforderungen erfüllen muss. Es gibt aber auch einige Voraussetzungen, die von einer Institution erfüllt werden sollten, damit ein IS-Webcheck gute Ergebnisse liefern kann.

2.1.1 Motivation für einen IS-Webcheck

Jede Institution kann ein Ziel von Angriffen werden und sollte daher über entsprechende Schutzmaßnahmen wie IS-Webchecks nachdenken. Von Behörden werden Aufträge nach außen vergeben, Gesetze erarbeitet und veröffentlicht, personenbezogene Daten verarbeitet, Steuern erhoben, Steuerrückzahlungen berechnet, Gesetzesverstöße verfolgt und vieles mehr. Nicht nur ein Datenverlust kann brisant sein, sondern auch der Imageschaden bei einem erfolgreichen Angriff.

Ebenso besitzen Unternehmen Know-How, auf dem der wirtschaftliche Erfolg des Unternehmens beruht. Auch hier kann ein Angriff fatale Folgen haben.

Wenn ein Angriff bereits erfolgt ist und der IS-Webcheck durchgeführt wird, um weitere Angriffsmöglichkeiten zu finden, sollte gewährleistet sein, dass eventuell notwendige Beweisaufnahmen abgeschlossen sind.

2.1.2 Rahmenbedingungen für IT-Sicherheitstests

IS-Webchecks müssen immer von fachlich qualifizierten Personen durchgeführt werden, die unabhängig von den untersuchten Bereichen sind und die nicht bei Konzeption, Aufbau oder Betrieb des untersuchten Informationsverbundes mitgewirkt haben. Auf der einen Seite soll so Betriebsblindheit verhindert werden, auf der anderen Seite Interessenkonflikten vorgebeugt werden. Daher sollte eine Institution für IS-Webchecks grundsätzlich externe Prüfer beauftragen. Es muss auch hierbei darauf geachtet werden, dass die extern beauftragten Prüfer frei von Interessenkonflikten sind und weder an Konzeption, Aufbau oder Betrieb des untersuchten Informationsverbundes mitgewirkt haben noch in Abhängigkeitsverhältnissen zu den Fachverantwortlichen stehen.

Beim Testen von IT-Systemen auf Sicherheit sollte ein mehrstufiges Verfahren vorgesehen sein. Wichtig bei neu aufgesetzten IT-Anwendungen ist, dass eine interne Qualitätssicherung stattgefunden hat. Ein IS-Webcheck oder ein IS-Penetrationstest kann die erforderliche Qualitätssicherung nicht ersetzen, da bei diesen Methoden keine funktionalen Aspekte betrachtet werden und sie nur stichprobenartig durchgeführt werden. Eine gute Qualitätssicherung ist so

vollständig wie möglich durchzuführen. Sie sollte auf reproduzierbaren Testverfahren basieren, welche bei jeder Änderung von IT-Komponenten erneut eingesetzt werden können.

Teil der Qualitätssicherung ist es, die Umsetzung der Sicherheitsmaßnahmen zu überprüfen. Dieser Aspekt kann durch interne oder externe Prüfer erledigt werden. Es muss aber gewährleistet sein, dass auch hier Unabhängigkeit und Unvoreingenommenheit bestehen. Wenn die Sicherheitsmaßnahmen nach Standards wie IT-Grundschutz [2] umgesetzt worden sind, dann können Instrumente wie die IS-Revision [1] zur Überprüfung eingesetzt werden. Eine Vollständigkeit wird über eine sogenannte IS-Querschnittsrevision erlangt; ein guter Überblick kann über eine IS-Kurzrevision gewonnen werden. Je nach Schutzbedarf der IT-Systeme wird hierbei auch eine Risikoanalyse durchgeführt, die beim IS-Penetrationstest oder IS-Webcheck helfen kann, das Prüfobjekt einzugrenzen, da hier die Wahrscheinlichkeit von Angriffen deutlicher wird.

IS-Webchecks dienen dazu, mit unabhängigem Blick weitere Angriffsmöglichkeiten zu finden und sollen helfen, die IT-Systeme weiter abzusichern. IS-Webchecks können in unterschiedlichem Umfang durchgeführt werden. Jeder umfangreiche Test bedeutet einen erheblichen Ressourcenaufwand bzgl. Kosten und Zeit sowohl für die beauftragten Prüfer als auch für die Mitarbeiter, die für den Betrieb und die Sicherheit der untersuchten Systeme verantwortlich sind. Es muss daher im Vorfeld abgewogen werden, welcher Sicherheitsgewinn mit einem IS-Webcheck durch welchen Aufwand erzeugt werden kann.

Das BSI empfiehlt, vor einem IS-Webchek zunächst eine IS-Kurzrevision [1] durchzuführen. Hierbei wird stichprobenartig die Basisabsicherung nach IT-Grundschutz [2] überprüft. Dabei werden auch Aspekte wie die Einbettung in die Infrastruktur oder organisatorische Fragen untersucht.

Beim IS-Webcheck sollte zunächst die Webanwendung ohne vorgeschaltetes Sicherheitsgateway untersucht werden. Hierbei wird überprüft, ob gängige Sicherheitslücken in der IT-Anwendung geschlossen sind und eine gute Eingabevalidierung vorliegt. Das Sicherheitsgateway sowie weitere Schnittstellen zu dem Webauftritt werden im letzten Schritt dann durch einen IS-Penetrationstest überprüft.

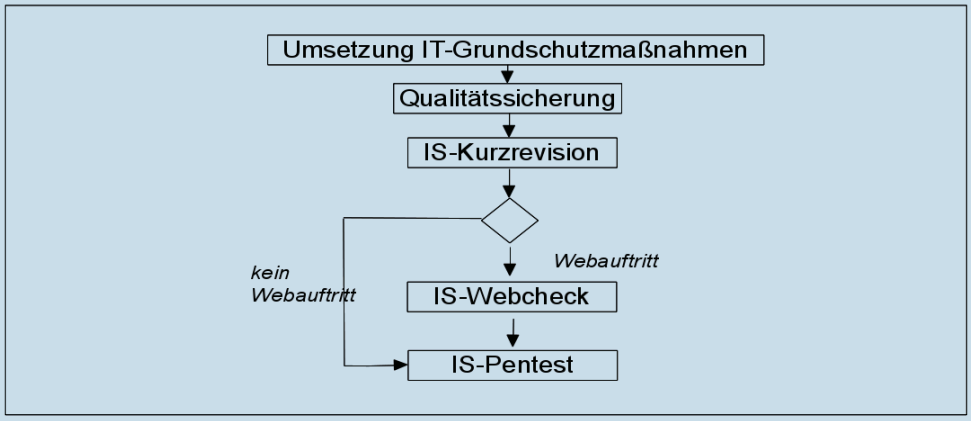


Abbildung 2: Reihenfolge der Sicherheitsmaßnahmen

2.2 Anforderungen an einen Prüfer

Ein Prüfer erhält Zugang zu vertraulichen Informationen über die Infrastruktur der getesteten Institution und deren Schwachstellen. Dies sollte den beauftragenden Institutionen bewusst sein. Bei der Suche nach einer vertrauenswürdigen Person/Firma für eine solche Aufgabe können die im Folgenden beschriebenen Kriterien herangezogen werden.

2.2.1 Fachliche Anforderungen

Die Prüfer müssen umfangreiche fachliche Kenntnisse haben. Werden die weiter unten beschriebenen Zertifikate vorgelegt, so kann von einer breiten fachlichen Qualifikation ausgegangen werden.

Wenn ein IS-Webcheck angestrebt wird, so sollten folgende Bereiche von den Prüfern beherrscht werden:

- allg. Prinzipien der Webentwicklung
- häufig verwendete Redaktionssysteme (Content Management Systeme) und Webanwendungsframeworks, Datenbanken, Webservices
- gängige in der Webentwicklung verwendete Programmier-/Skriptsprachen und PlugIns
- Internetprotokolle und im Internet verwendete Kommunikationsstandards
- Webserver und häufig verwendete Webservermodule
- spezielle IT-Sicherheits- und Lastverteilungsprodukte für Webauftritte (Web Application Firewalls, Reverse Proxy, Loadbalancer)

Es ist hilfreich, wenn ein Prüfer für IS-Webchecks selbst schon im Bereich Webadministration oder Webentwicklung gearbeitet hat, da er hierdurch Erfahrung mit möglichen Fehlerquellen mitbringt.

2.2.2 Weitere Fähigkeiten

Um eine vertrauensvolle Person für IS-Webchecks zu finden, sind neben den technischen Kenntnissen auch weitere Fähigkeiten sehr wichtig.

Ein Prüfer sollte folgende Qualitäten besitzen:

- Organisatorische Fähigkeiten
- Zielorientiertes Denken und Handeln
- Überzeugungsfähigkeit
- Schnelle Auffassungsgabe
- Gesundes Urteilsvermögen
- Analytische Fähigkeiten
- Teamfähigkeit

- Belastbarkeit
- Sachlichkeit insbesondere bei heiklen Sachverhalten

Die aufgezählten Fähigkeiten lassen sich nicht einfach nachweisen. Bei der Beauftragung einer Person, einen IS-Webcheck durchzuführen, muss sich die Institution daher bei diesen Punkten teilweise auf die eigene Intuition und die Erfahrungen mit dem Auftragnehmer verlassen.

Einige Anhaltspunkte lassen sich jedoch aus den Angeboten herauslesen. Beispielsweise können anhand der Referenzen Rückschlüsse gezogen werden. Es ist aber auch möglich, dass der Anbieter keine Referenzen vorlegen kann, weil die geprüften Institutionen einer Nennung nicht zugestimmt haben. Gerade bei IT-Sicherheitstests nach erfolgreichen Angriffen herrscht eine größere Verschwiegenheit. Hierbei kann es nützlich sein, sich bestätigen zu lassen, in welchen Branchen ein Anbieter gearbeitet hat und welche Unternehmensgröße bereits getestete Institutionen hatten.

Ein sehr wichtiger Punkt ist die Unabhängigkeit und die Neutralität der Prüfer. Steht ein Prüfer in einem Abhängigkeitsverhältnis zu der getesteten Institution, so verliert er die notwendige Unabhängigkeit, die für jede Art von IT-Sicherheitstests notwendig ist. Ein Prüfer muss die Möglichkeit besitzen, ohne Konsequenzen für sich, auch sehr negative Aspekte für die getestete Institution ansprechen zu können.

Dies schließt aus, dass IT-Sicherheitstests von eigenem Personal durchgeführt werden. Es können einzelne Testverfahren eines IS-Penetrationstests oder IS-Webchecks im eigenen Haus angewandt werden, um Schwachstellen aufzuspüren, aber der eigentliche IT-Sicherheitstest sollte immer von einem Externen durchgeführt werden.

Ein weiterer Grund für die Verwendung von Externen ist die notwendige Unvoreingenommenheit des Prüfers. Nur wenn ein Prüfer weder in die Organisationsstrukturen der Institution eingebunden ist, noch bei Konzeptionierung oder Betrieb der zu untersuchenden IT-Systeme mitgewirkt hat, kann er einen unvoreingenommenen Blick auf die zu testenden IT-Systeme haben, der notwendig ist, um auch ausgefallene Angriffsmöglichkeiten oder Schwächen im Konzept zu entdecken. Nur so ist es möglich, dass er unabhängig auf Konfigurationsmängel hinweisen kann, die Sicherheitslücken darstellen, aber vielleicht im IT-Betrieb als sinnvoll angesehen wurden.

Das BSI empfiehlt, dass ein Testteam bestehend aus mindestens zwei Personen für einen IS-Webcheck eingesetzt wird, damit das Vier-Augenprinzip gewahrt bleibt. Letztendlich entscheidet der Kostenfaktor, wie viele Personen beauftragt werden. Es muss insbesondere bei kleinen Prüfobjekten zwischen Kosten und Nutzen abgewogen werden.

2.2.3 Technische Qualifikation / Zertifikate

Anbieter, die IS-Webchecks anbieten, sollten möglichst als Prüfstelle zertifiziert sein. Sie sollten nachweislich die Grundsätze des Datenschutzes, der sicheren Datenhaltung und der IT-Sicherheit einhalten und qualifiziertes Personal beschäftigen.

Nachgewiesen werden kann die fachliche Qualifikation über Zertifikate für Prüfstellen oder auch über Zertifikate für das Personal wie beispielsweise über die Personenzertifizierung des BSI [4] oder CREST [5]. Beide Verfahren enthalten praktische Prüfungen, womit die Fähigkeit zur Umsetzung eines IT-Webchecks geprüft wird. Ebenfalls weit verbreitet sind Zertifikate wie der Certified Ethical Hacker [6], wo in theoretischen Prüfungen nachgewiesen wird, dass entsprechende Fähigkeiten vorhanden sind. Da bei dem Certified Ethical Hacker und den dazu gehörenden

Aufbauzertifikaten ein umfangreiches Wissen abgefragt wird, können auch diese Zertifikate als Befähigungsnachweis herangezogen werden.

Sollte kein Zertifikat für die Prüfstelle bzw. deren Personal vorliegen, so *empfiehlt das BSI*, folgende Voraussetzungen des BSI-Personenzertifikats für die Projektleitung auf Prüfseite heran zu ziehen. Es wird dort verlangt, dass der hauptverantwortliche Prüfer Berufserfahrung in dem Bereich IT-Penetrationstest besitzt und eine technische Ausbildung abgeschlossen hat. Der Projektverantwortliche muss in den letzten acht Jahren mindestens fünf Jahre Berufserfahrung (Vollzeit) im Bereich IT erworben haben, davon sollten mindestens zwei Jahre (Vollzeit) im Bereich Informationssicherheit absolviert worden sein. Zudem sollte der Prüfer an mindestens sechs Penetrationstests in den letzten drei Jahren teilgenommen haben. Dies sollte möglichst vom Anbieter über entsprechende Referenzen nachgewiesen werden.

2.2.4 Verwendete Tools

Die Prüfer sollten die bei IS-Webchecks eingesetzten Werkzeuge sorgfältig auswählen. Im Internet sind viele freie Programme zu finden, die für IS-Webchecks eingesetzt werden können. Daneben gibt es kommerzielle Programme, die sehr teuer sind, weshalb häufig die freien Tools bevorzugt werden. Viele der freien Tools sind gut und es spricht nichts gegen deren Einsatz. Es muss aber beachtet werden, dass einige Programme (frei oder kommerziell) sehr speziell auf Anwendungsfälle zugeschnitten worden sind und durch einen falschen Einsatz etwas zerstören können. Der Vorteil bei den kommerziellen Tools ist, dass diese häufig besser dokumentiert sind. Wichtig bei der Auswahl ist, dass der Prüfer die verwendeten Tools mit allen Einsatzgebieten genau kennt und getestet hat.

2.3 Weitere Rahmenbedingungen

Die folgenden Rahmenbedingungen müssen bei einem IS-Webcheck beachtet werden. Der Institution sollte bewusst sein, dass ein IS-Webcheck möglicherweise Daten betrifft, die gesetzlichen Regularien unterliegen.

Verträge

Die Prüfer bzw. die Prüfstellen sollten nie ohne schriftlichen Auftrag eine IT-Anwendung testen. Daher sollte immer ein Vertrag zwischen Prüfern und getesteter Institution geschlossen werden. Sind Dienste bei einem Hoster ausgelagert, so muss auch dieser in den Vertrag einbezogen werden.

Der Vertrag sollte Rahmenbedingungen wie Prüfzeitraum, Prüfobjekt und Prüftiefe spezifizieren. Hierdurch kann vermieden werden, dass Prüfer unbeabsichtigt zu tief testen oder IT-Systeme beeinflussen, die nicht beeinträchtigt werden dürfen. Andererseits können auch die Prüfer dagegen geschützt werden, dass nicht zufällig während der IS-Webchecks aufgetretene Fehler an anderen IT-Systemen auf sie bezogen werden.

Es sollte festgelegt werden, welche Kosten anfallen werden und was neben dem Test selbst erwartet wird, wie zum Beispiel eine Präsentation vor dem Management oder ein besonders umfangreicher Bericht. Außerdem müssen die Mitwirkungspflichten des Auftraggebers festgelegt werden.

Es sollten weiterhin Vereinbarungen bezüglich der Haftbarkeit und der Verschwiegenheit getroffen werden.

Der Vertrag sollte beinhalten, dass die gefundenen Ergebnisse nur zum Zeitpunkt des IS-Webchecks gültig sind und bei eventueller Beschränkungen der zeitlichen, finanziellen und personellen Ressourcen nicht gewährleistet ist, dass alle vorhandenen Fehler gefunden werden.

NDA (Non Disclosure Agreement)

Im Vertrag solte festgelegt werden, dass weder über die vorgefundenen Sicherheitsmängel, noch über die Organisationsstrukturen und die Struktur der überprüften IT-Systeme, noch über gesichtetes Firmen-Know-How gegenüber Dritten kommuniziert wird.

Es kommt vor, dass Prüfer Berichte über gefundene Schwachstellen veröffentlichen, um die Öffentlichkeit dafür zu sensibilisieren. Dies ist wichtig, da aus den Fehlern auch Dritte lernen können. Hierbei muss gewährleistet sein, dass die Daten anonymisiert sind und kein Rückschluss auf die getestete Institution gezogen werden kann.

Speicherzeit von Daten

Die Prüfer müssen während der praktischen Tests Daten speichern, durch deren Auswertung sie erst einen Bericht erstellen können. Es sollte vor einem IS-Webcheck vereinbart werden, welche Daten in welcher Form und auf welchen Datenträgern erhoben werden und nach welcher Zeit die Prüfer die erhobenen Daten löschen müssen und welche Nachweise dafür zu erbringen sind.

Datenschutz

Der Datenschutz muss zu jeder Zeit gewährleistet bleiben. Wenn personenbezogene Daten von einem IS-Webcheck betroffen sind, so muss der Datenschutzbeauftragte und gegebenenfalls auch die Personalvertretung der beauftragenden Institution vor den Tests einbezogen werden. Es muss geklärt werden, zu welchem Zweck der IS-Webcheck durchgeführt wird und vertraglich vereinbart werden, wie Daten anonymisiert werden können. Auch sollten besonders diese Daten nach Auswertung der Testergebnisse gelöscht werden.

Geheimschutz

Wenn als Verschlusssache (VS) eingestufte Informationen oder VS verarbeitende IT-Systeme durch einen IS-Penetrationstest betroffen sind, ist die für den Geheimschutz zuständige Stelle zu beteiligen. Sie legt die Mittel und Wege fest, wie der IS-Penetrationstest nach den VS-Vorschriften durchzuführen ist. Die Prüfer müssen entsprechend der VS-Einstufung sicherheitsüberprüft sein und zum Zugang zu VS ermächtigt werden.

Benachrichtigung von betroffenen Personen (IT-Sicherheitsbeauftragter, Kunden, Mitarbeiter)

Zunächst muss sichergestellt werden, dass der IT-Sicherheitsbeauftragte, sofern die Institution über einen solchen verfügt, informiert und einbezogen ist.

Durch die IS-Webchecks können aber auch Personenkreise außerhalb des untersuchten Bereichs betroffen sein. Durch die IS-Webchecks kann es beispielsweise zu einer erhöhten Netzwerkauslastung kommen, die Mitarbeiter oder Kunden in ihrer normalen Arbeit beeinträchtigt. Die IS-Webchecks sollten daher so geplant werden, dass möglichst wenig Beeinträchtigungen stattfinden. Außerdem ist es ratsam, die betroffenen Personenkreise vor einem IS-Webcheck zu benachrichtigen, um unnötigen Unmut zu vermeiden.

Wartung der IT-Systeme

Wenn die Zeiträume zur Durchführung von IS-Webchecks ausgewählt werden, sollte darauf geachtet werden, dass nicht gleichzeitig Wartungsarbeiten an den betroffenen IT-Systemen durchgeführt werden. Manchmal werden die Planungen von unterschiedlichen Abteilungen durchgeführt, sodass es zu Überschneidungen kommen kann. Ein IS-Webcheck auf ein IT-System, welches gerade verändert wird, verliert an Aussagekraft.

3 Fachliche Voraussetzungen für einen IS-Webcheck

Um die Zeit während eines IS-Webcheck so effektiv wie möglich zu nutzen, sollten einige Vorbereitungen getroffen werden.

3.1 Festlegung des Prüfobjekts zwischen Prüfer und Institution

Die Institution und der Prüfer sollten genau festlegen, welche Bereiche des Webangebots getestet werden. Oftmals sind die Webangebote weit verzweigt, wobei jeder Zweig über eigene URLs erreichbar ist. Hierbei empfiehlt sich, auf Basis der identifizierten Bedrohungslage und dem Schutzbedarf der Geschäftsprozesse und Informationen diejenigen Webanwendungen in den Fokus zu nehmen, die besonders geschäftskritisch sind.

Üblicherweise wird nach einer Erstinbetriebnahme einer Webanwendung oder wesentlichen Änderungen ein IS-Webcheck angestrebt oder auch, wenn ein Angriff bereits stattgefunden hat. Hierbei kann das Prüfobjekt meistens leicht eingegrenzt werden.

Wenn eine Institution präventiv einen IS-Webcheck durchführen möchte, so fällt es oft schwer, das Prüfobjekt einzugrenzen, vor allem wenn eine Institution über zahlreiche Webauftritte verfügt. Die Institution möchte jede Angriffsmöglichkeit identifizieren und beseitigen. Dies ist allerdings sehr zeitaufwendig und teuer. Oft steht auch kein Prüfer für eine so lange Zeitspanne zur Verfügung. Daher sollte gemeinsam mit dem Prüfer überlegt werden, wo ein Angriff am wahrscheinlichsten ist und die identifizierten Webanwendungen vorgezogen werden. Es können in der Folgezeit sukzessive weitere IS-Webchecks auf weitere Webanwendungen durchgeführt werden. Da Prüfer keine Qualitätssicherung übernehmen können und Betriebsblindheit vermieden werden muss, sollten die jeweiligen Webanwendungen nicht mehrfach von denselben Prüfern überprüft werden.

Es muss darüber hinaus festgelegt werden, ob interne zugriffsgeschützte Bereiche mit getestet werden sollen. Dann müssen den Prüfern Zugangsdaten und wenn notwendig Token oder Zertifikate zur Verfügung gestellt werden.

> *Das BSI empfiehlt*, alle zwei bis drei Jahre Wiederholungsprüfungen durchzuführen, da regelmäßig neue Schwachstellen und Angriffsmethoden bekannt werden.

3.2 Festlegung des Prüfumfangs

Wenn das Prüfobjekt festgelegt ist, sollte der Prüfumfang definiert werden.

Hierbei werden folgende Aspekte vereinbart:

- Prüftiefe
- Prüfort
- Prüfzeitraum
- Prüfbedingungen

Prüftiefe

Bei IS-Webchecks gibt es nur zwei unterschiedliche Prüftiefen. Die Möglichkeit, ein *technisches Sicherheitsaudit* wie bei einem herkömmlichen IS-Penetrationstest durchzuführen, gibt es hier nicht, da die Prüfer in der Regel nicht vor Ort sind.

Ein *nicht invasiver Schwachstellenscan* ist die erste mögliche Prüftiefe. Hierbei scannt der Prüfer mit einem Schwachstellenscanner und manuellen Methoden die Webanwendung auf Schwachstellen. Bei einem IS-Penetrationstest werden bei dieser Prüftiefe die Schwachstellen nicht ausgenutzt. Bei einem IS-Webcheck muss hier differenziert werden, ob die Schwachstellen sich auf Interaktionsmöglichkeiten des Anwenders beziehen oder auf Schwachstellen in der eingesetzten Software. Die Schwachstellen bei den Interaktionsmöglichkeiten des Anwenders wie Eingabefelder, Formularfelder oder Click-Buttons bzw. teilweise bei den Zugriffen auf die Anwendungen und Datenbanken hinter der der Webanwendung sind ohne Ausnutzen der Schwachstelle nicht nachweisbar. Hier sollte darauf geachtet werden, dass die Schwachstellen nur auf harmlose nicht invasive Weise ausgenutzt werden.

In der nächsten Prüftiefe beim *invasiven Schwachstellenscan* werden zusätzlich so genannte *Exploits* eingesetzt. Das sind Programme, die eigens zum Ausnutzen von bekannten Schwachstellen geschrieben wurden. Hierdurch wird nachgewiesen, an welchen Stellen die Webanwendung auf welche Art angreifbar ist. Die Exploits können teilweise einen unkalkulierbaren Schaden anrichten, wenn sie nicht gezielt für die vorliegende Anwendung geschrieben wurden. Da keine Anwendung der anderen gleicht, weil die Konfigurationen und Einstellungen unterschiedlich sind, können frei verfügbare Exploits die IT-Systeme stark beeinträchtigen.

> Bei der Festlegung der Prüftiefe sollte eine Abwägung getroffen werden, was den meisten Nutzen verspricht. *Das BSI empfiehlt*, eine moderate Angriffsstärke auszuwählen und mit Schwachstellenscannern mögliche Lücken zu identifizieren und wenn überhaupt nur bei genau getesteten Exploits, diese auch einzusetzen.

Da ein echter Angreifer nicht vor aggressiven Methoden zurückschreckt, muss bei Festlegung der Prüftiefe in jedem Fall abgewogen werden, ob nicht vereinzelt aktiv Exploits eingesetzt werden sollen, um die Schwächen der Webanwendung zu finden. Es ist besser, unter kontrollierten Bedingungen Abstürze zu provozieren als wenn bei einem tatsächlichen Angriff ein unkontrollierter Absturz zu Datenverlust führt. Bei Einsatz solcher Methoden sollte aber in jedem Fall eine gute Backup-Strategie vorhanden sein, wenn an den Originalsystemen getestet wird.

Prüfort

Schließlich muss noch der Ort festgelegt werden, wo der IS-Webcheck stattfindet. Bei einem herkömmlichen IS-Webcheck wird dies das Prüflabor der Prüfer sein.

Wenn die Webanwendung nicht über das Internet angeschlossen ist, ist der Ort gegebenenfalls anders zu wählen. Wenn eine Intranetanwendung getestet wird, so kann beispielsweise der Prüfer mit einem Laptop innerhalb des Netzes der Institution testen.

Prüfbedingungen

Wenn der Ort des IS-Webchecks festgelegt ist, muss genau geplant werden, welche Bedingungen der Auftraggeber für den Prüfer einplanen muss.

Der Institution und eventuell beteiligten Hostern muss der Netzwerkadressbereich, aus dem der Zugriff erfolgt, mitgeteilt werden. Einerseits können die Institution bzw. die Hoster damit zum Zeitpunkt des Tests unterscheiden, ob die Zugriffe zu den Testangriffen zählen oder ob zufälligerweise ein 'echter' Angriff parallel stattfindet. Darüber hinaus ist es auch Aufgabe der Institution bzw. des Hosters den Zugriff auf die Webanwendung für den Zeitraum der Tests durch das Sicherheitsgateway freizugeben. Dies dient dazu, exakte Ergebnisse bzgl. der getesteten Webanwendung zu erhalten. Wenn das Sicherheitsgateway zusätzliche Absicherungen bereithält, ist das für den Betrieb gut. Ein genaues Prüfergebnis, wo welche Schwächen zu beseitigen sind, kann der Prüfer leichter und somit kostengünstiger erzeugen, wenn die IT-Systeme getrennt voneinander getestet werden. Die Funktion des Sicherheitsgateways sollte dann in einem separaten IS-Penetrationstest getestet werden.

Wenn ein IS-Webcheck nicht auf dem Originalsystem stattfinden kann, kann eine Simulation getestet werden. Dies trifft beispielsweise zu, wenn eine revisionssichere Archivierung zu testen ist, bei der selbst Testdaten nicht ohne Weiteres gelöscht werden dürfen. Hierbei liegt es in der Verantwortung der Institution, dass die verwendeten IT-Systeme identisch aufgebaut sind. Es muss allerdings hierbei beachtet werden, dass die gefundenen Ergebnisse sich nur auf das getestete Prüfobjekt beziehen und nur bedingt auf das Originalsystem übertragen werden können.

Wenn Bereiche mit unterschiedlichen Rechten getestet werden sollen, muss für jeden Bereich mindestens ein Testzugang angelegt werden. Der Prüfer sollte sich auch auf diesen Zugang beschränken, um der Institution das Aufräumen nach dem Test zu erleichtern. Alle zu dem Testzugang gehörenden Daten können auf diese Weise leicht wieder gelöscht werden.

Der Auftraggeber sollte gewährleisten, dass keine Änderungen an den Systemen während der Tests durchgeführt werden. Sollte der Ansprechpartner des Auftraggebers durch Beobachten des IS-Webchecks oder Gespräche auf Sicherheitslücken aufmerksam werden, so muss er warten, bis der IS-Webcheck abgeschlossen ist, bevor er die Lücke beseitigt, da sonst die Testergebnisse verfälscht werden können. Sollte eine so gravierende Lücke entdeckt werden, dass es unabdingbar ist, diese sofort zu schließen, so sollte der IS-Webcheck abgebrochen und zu einem späteren Zeitpunkt fortgeführt werden.

Prüfzeitraum

Es ist wichtig, vor jedem IS-Webcheck einen genauen zeitlichen Rahmen für die Durchführung festzulegen, damit einerseits die Institution den IS-Webcheck genau vorbereiten und planen kann und andererseits der Prüfer eine Vorgabe hat. Es sollte ausreichend Einarbeitungszeit in die zu untersuchende Technik und auch Zeit für die Berichterstellung eingeplant werden.

3.3 Dokumentation

Damit die Prüfer bei einem Whitebox-Test einen schnellen Überblick über die zu testenden Prüfobjekte erhalten, sollten die im Folgenden aufgelisteten Unterlagen vom Auftraggeber zur Verfügung stehen.

- **Zieladresse der Webanwendung und Zugangsdaten**

  Die Zieladresse der Webanwendung sollte den Prüfern als URL und IP-Adresse mitgeteilt werden. Zusätzlich sollten den Prüfern für alle Testzugänge die Zugangsdaten und ggf. notwendige Token oder Zertifikate zur Verfügung gestellt werden.

- **kurze Beschreibung des Prüfobjekts**

  Eine Dokumentation des Prüfobjekts sollte vorliegen. Hierbei soll beschrieben werden, wofür das Prüfobjekt benötigt wird. Die Dokumentation soll mindestens beschreiben, welche Teilnehmer Zugriff auf das Objekt besitzen, zu welchen Zeiten Zugriffe erfolgen, welche Daten personenbezogen sind oder ggf. nach Geheimschutz zu behandeln sind.

  Die Webanwendung selbst sollte in klar abgegrenzte Funktionen unterteilt und diese beschrieben werden. Beispielsweise könnte das Prüfobjekt die vollautomatische Anmeldung von Teilnehmern zu einer Veranstaltung per E-Mail sein. Die Funktionen können Mailempfang, Verarbeitung der E-Mail, Empfangsbestätigung und Statusmeldung sein. Beim Mailempfang muss beschrieben werden, welcher Teilnehmerkreis berechtigt ist, Anmeldungen zu schicken, ob ein Anmeldeformular als Anhang erwartet wird und wie unberechtigte E-Mails herausgefiltert werden. Wenn ein Anmeldeformular erwartet wird, muss erkennbar sein, wie dieses aufgebaut ist und welcher MIME-Type erwartet wird. Bei der Verarbeitung könnte überprüft werden, ob noch ausreichend Plätze vorhanden sind und bei der Empfangsbestätigung könnte eine Bestätigung oder Absage verschickt werden.

  Spezielle Sicherheitsmaßnahmen bezüglich der Webanwendung selbst sollten beschrieben werden. Bei obigem Beispiel könnte das beinhalten, welche Personen Zugriff auf die IT-Systeme haben und mit welchen Maßnahmen verhindert wird, dass unberechtigte Personen über die Webanwendung an die IT-Systeme gelangen.

- **Liste der beteiligten IT-Systeme mit Beschreibung der Härtungsmaßnahmen**

  Darüber hinaus sollten alle beteiligten IT-Systeme (Webserver, Datenbank, Anwendungssysteme) mit der eingesetzten Betriebssystemversion und Version der Anwendungssoftware bzw. Datenbankversion dokumentiert sein. Alleine die Auseinandersetzung der Institution mit diesem Thema führt dazu, dass veraltete Dienste bereits identifiziert und gepatcht werden können. Die Härtung der IT-Systeme wird bei einem IS-Webcheck nicht getestet, dies kann in einem separaten IS-Penetrationstest durchgeführt werden.

- **Beschreibung der Kommunikationsverbindungen (ggf. als Netzplan)**

  Alle notwendigen Kommunikationsverbindungen sollten nachvollziehbar dokumentiert sein. Es sollte nicht möglich sein, weitere Kommunikationsverbindungen aufzubauen. Es sollte beschrieben werden, was für IT-Sicherheitsvorkehrungen getroffen wurden, damit nur zulässige Verbindungen aufgebaut werden können.

Um die Testzeit vor Ort so gering wie möglich zu halten, sollten die Unterlagen im Vorfeld an die Prüfer übergeben werden, damit sich diese einarbeiten können.

3.4 Verantwortlichkeiten

Schließlich müssen noch die Verantwortlichen auf beiden Seiten festgelegt werden, die bei einem IS-Webcheck zur Verfügung stehen müssen.

Hierbei sollte gewährleistet sein, dass die Prüfer auch tatsächlich auf die IT-Systeme vor Ort spezialisiert sind. Der Auftraggeber sollte darauf achten, dass die Personen den IS-Webcheck durchführen auch über die im Angebot beschriebenen Qualifikationen verfügen. Es sollten nur Vertreter akzeptiert werden, wenn diese vergleichbare Qualifikationen nachweisen können.

Für den Prüfzeitraum sollte immer auch von der Seite der Institution bzw. des Hosters mindestens ein Ansprechpartner für die Prüfer zur Verfügung stehen, der zu dem Prüfobjekt Auskunft geben kann. Weitere Techniker, die tiefere Fragen klären könnten, sollten während der Tests in Bereitschaft sein. Ersatzweise müssen Zeiten festgelegt werden, wann diese befragt werden können.

4 Ablauf eines IS-Webchecks

Im Folgenden wird, soweit es möglich ist, der praktische Ablauf eines IS-Webchecks beschrieben. In den meisten Fällen werden vor allem im praktischen Teil weitere Aspekte hinzukommen, die aber individuell auf das Prüfobjekt bezogen festgelegt werden.

Es werden an dieser Stelle Module beschrieben, die aus Sicht des BSI bei einem IS-Webcheck mindestens abgearbeitet werden sollten. Die Teilaspekte der Module sind sehr umfangreich, da die Möglichkeiten der Gestaltung von Webanwendungen umfangreich sind. Für eine detaillierte Beschreibung der verschiedenen Möglichkeiten wird an dieser Stelle auf die Testrichtlinien von OWASP [12] und das Web Application Hackers Handbook [11] von Dafydd Stuttard und Marcus Pinto hingewiesen, wo sehr ausführliche Checklisten sowie gute Beschreibungen der Methoden zu finden sind.

4.1 Einarbeitung der Prüfer

Das erste Arbeitspaket des IS-Webchecks sollte der Einarbeitung der Prüfer dienen. Ein versierter Prüfer benötigt möglicherweise weniger Zeit, wenn er die Art der Webanwendung gut kennt. Für ausgefallenere Webanwendungen wird meist mehr Zeit benötigt. Die Institution muss den Prüfern für die Einarbeitung eine ausführliche Dokumentation (siehe Kapitel 3.2) zur Verfügung stellen.

4.2 Test des Prüfobjekts

Das nächste größere Arbeitspaket eines IS-Webchecks ist der Test des Prüfobjekts. Es wird empfohlen, den Test in folgende Arbeitspakete aufzuteilen

- Anfangsgespräch
- Einrichten der Arbeitsumgebung
- Praktische Prüfung
- Abschlussgespräch

Je nach Umfang des Tests können außerdem verschiedene Zwischengespräche notwendig sein oder einzelne Pakete wie Einrichten der Arbeitsumgebung und die praktische Prüfung mehrfach durchgeführt werden. Nach Abschluss der Arbeiten sollte eine kurze Zusammenfassung erfolgen.

Anfangsgespräch

Am ersten Tag sollte vor Beginn der Tests ein kurzes Gespräch mit dem Auftraggeber/Hoster und dem beteiligten technischen Personal stattfinden. Da der IS-Webcheck nich vor Ort durchgeführt wird, wird das Gespräch per Telefon durchgeführt. Es empfiehlt sich noch einmal das Prüfobjekt und das Prüfmodul zu besprechen, um sicherzustellen, dass alle Beteiligten die gleichen Vorstellungen vom Prüfobjekt und Umfang der Tests besitzen. Eventuelle Missverständnisse können hier noch einmal aus dem Weg geräumt werden.

Prüfbedingungen

Danach werden die Prüfbedingungen für den Test in Augenschein genommen. Die Prüfer klären, ob die besprochenen Voraussetzungen für den Test erfüllt sind. Anschließend testen die Prüfer, ob der

Zugang zu den IT-Systemen wie abgesprochen möglich ist und stellen fest, ob die Ansprechpartner auskunftsfähig sind.

Praktische Prüfung

Im Folgenden werden einige wiederkehrende Elemente beschrieben, die grundsätzlich im praktischen Teil eines IS-Webchecks vorkommen. Die im Folgenden beschriebenen Module sollen einen Überblick über die Kernelemente eines IS-Webchecks liefern. Beim Test selbst muss jederzeit die Möglichkeit offengehalten sein, über diese Kernelemente hinauszugehen, wenn ein Angriff auf anderem Weg möglich ist.

Die Aufteilung in die Module wurde vorgenommen, um Außenstehenden einen Überblick über die getetesten Aspekte zu vermitteln. Die Reihenfolge der Module kann individuell festgelegt werden, auch können einzelne Module mehrfach durchgeführt oder gleichzeitig abgearbeitet werden. Dies geschieht beispielsweise, wenn in einem Modul die Ergebnisse für einen Teiltest eines anderen Moduls geliefert werden. Sollte ein Teiltest nicht durchgeführt werden, so sollte für Prüfer und Auftraggeber nachvollziehbar sein, warum dies nicht erfolgt ist.

Um die Auswertung zu erleichtern, sollte eine ausführliche Dokumentation während der praktischen Prüfung erfolgen. Wenn einzelne Aspekte nicht getestet werden, sollte dies nachvollziehbar begründet werden.

Modul 1 – Schwachstellensuche

In diesem Modul wird Mithilfe der Dokumentation aber auch an Hand des Verhaltens der Webanwendung (beispielsweise aus Fehlermeldungen oder dem Antwortverhalten des Webservers) zusammengetragen, welche Softwareversionen bei dem Webserver, den Anwendungen und den Datenbanken eingesetzt werden. Anhand der Aktualität der Versionen kann auf mögliche vorhandene Schwachstellen geschlossen werden.

Es wird geprüft, ob eine Verschlüsselung eingesetzt wird und ob diese den aktuellen Sicherheitsanforderungen entspricht. Wenn keine Verschlüsselung eingesetzt wird, wird an dieser Stelle geprüft, ob die verarbeiten Daten auch tatsächlich offen sind und keiner weiteren Absicherung bedürfen.

Mit der Dokumentation wurde den Prüfern schon ein Überblick verschafft, was die Webanwendung leisten soll und welche Funktionen erfüllt werden. Zu den erwarteten Funktionen werden die Interaktionsmöglichkeiten in der Webanwendung gesucht.

Viele Webanwendungen liefern zunächst ein großes Informationsangebot, aber auch viele Interaktionsmöglichkeiten mit der Anwendung, wie beispielsweise eine Suchfunktion oder ein Kontaktformular mit E-Mailversand. Häufig werden aber auch umfangreiche Funktionen wie Webshops, Diskussionsforen, Dateiaustausch und vieles mehr angeboten.

Jede Möglichkeit eines Anwenders Eingaben zu tätigen oder Aktionen durchzuführen, beinhaltet die Möglichkeit der Beeinflussung des Webangebots. Wenn eine gute Absicherung implementiert ist, dann ist höchstwahrscheinlich nur erwünschtes Verhalten zugelassen, bei schlechterer Absicherung sind hier die möglichen Angriffspunkte zu finden. Diese Möglichkeiten sollen an dieser Stelle identifiziert und in den folgenden Modulen genauer untersucht werden.

Aber auch Parameter die nicht offensichtlich zu den Interaktionen gehören, können veränderbar sein und damit das Verhalten der Webanwendung beeinflussen. Beispielsweise könnte in der URL der Parameter „user=anwender“ nach erfolgreicher Anmeldung übergeben werden und dann beim Surfen durch das Angebot mitgeführt werden. Eine Veränderung des Parameters in „user=administrator“ könnte dem Anwender bei mangelnder Absicherung unerwünschte

Zugriffsrechte bescheren. Auch solche Parameter werden an dieser Stelle gesucht, um hierüber weitere Angriffsmöglichkeiten zu entdecken.

Bei automatisierten Methoden muss beachtet werden, dass viele "False Positives" gemeldet werden, also fälschlich Sicherheitslücken identifiziert werden, die nicht vorhanden sind. Die meisten Webanwendungsscanner entscheiden beispielsweise anhand der Antwort der Webanwendung, ob eine Schwachstelle vorliegen kann. Manche Anwendungen sind allerdings so konzipiert, dass sie keine Fehlermeldungen herausgeben, sondern im Fehlerfall auf die Hauptseite oder eine Suchseite umleiten. Dann gewinnt ein automatisierter Schwachstellenscanner den Eindruck, dass Seiten vorhanden sind, die nicht da sind. Auch werden einige Schwachstellen übersehen, weil die Intelligenz der Scanner nicht ausreicht, Rückschlüsse aus Ergebnissen zu ziehen und darauf weitere Tests aufzusetzen. Jeder automatisierte Scan muss also durch manuelle Methoden verifiziert und erweitert werden.

Modul 2 – Schwachstellentest

In diesem Modul wird festgestellt, ob die für das Prüfobjekt erforderlichen Härtungsmaßnahmen umgesetzt sind. Hierbei werden die Erkenntnisse aus Modul 1 herangezogen und auf Angreifbarkeit überprüft. Es wird empfohlen, dass die Tests sowohl automatisiert als auch manuell durchgeführt werden.

Hierbei sollten mindestens folgende Punkte überprüft werden:

- Eingabevalidierung
- Session Handling
- Zugriffskontrolle
- Verschlüsselung
- Fehlerhandling
- Absicherung der beteiligten Datenbanken und Anwendungen
- Absicherung von Dateiuploadmöglichkeiten und weiteren Interaktionsmöglichkeiten
- versteckte Parameter/Verzeichnisse

Es kommen je nach Webanwendung weitere individuelle Punkte hinzu, die aus den Dokumentationen der Webanwendung selbst erarbeitet werden müssen.

Im folgenden werden die zu überprüfenden Punkte beispielhaft erläutert, damit das Prinzip klar wird. Es gibt zahlreiche weitere Möglichkeiten, die von Fall zu Fall individuell getestet werden müssen. Gute Anleitungen für Webanwender für eine erfolgreiche Absicherung aber auch für Prüfer, welche Aspekte getestet werden sollten, finden sich in den Testrichtlinien von OWASP [12] und dem Web Application Hackers Handbook [11] von Dafydd Stuttard und Marcus Pinto und werden an dieser Stelle nicht ausführlich beschrieben.

Eingabevalidierung

Jedes Eingabefeld, in das der Anwender Eingaben tätigen kann, wurde dafür konzipiert, Daten an die Anwendung und die ggf. dahinter liegenden Datenbanken weiterzugeben. Wenn die Eingabe nicht ausreichend abgesichert ist, können hierüber Angriffe getätigt werden. Der bekannteste Angriff dieser Art ist die so genannte 'Cross-Site-Scripting'-Attacke. Hierbei wird statt der normalen Eingabe Skriptcode in das Eingabefeld eingegeben. Da meist nach erfolgreicher Eingabe von Daten, die Daten vom Client noch einmal angezeigt werden und die meisten Browser so konfiguriert sind,

dass sie Scriptcode ausführen und das Ergebnis darstellen, kann ohne entsprechende Absicherung bei Eingabe von Skriptcode in ein Eingabefeld ein großer Umfang von Funktionen zur Ausführung gebracht werden, ohne dass der Anwender dies bemerkt. Wenn eine solche Eingabe ohne entsprechende Absicherung beispielsweise in einem Gästebuch eingegeben wird, wird das Skript bei jedem Anwender, der diese Seite besucht, ausgeführt.

Aber auch angeschlossene Datenbanken können bei mangelnder Absicherung betroffen sein. So könnte beispielsweise ein Datenbankbefehl an die dahinter liegende Datenbank weitergegeben werden und damit Daten der Datenbank sichtbar gemacht, gelöscht oder verändert werden, die nicht für den Zugriff des Anwenders gedacht waren.

Zusätzlich kann, wenn die Länge der Eingabe nicht ausreichend geprüft wird, möglicherweise die Anwendung hinter der Webseite oder das System des Anwendungsservers zum Absturz gebracht werden.

Session Handling

Webanwendungen sind im Regelfall so konzipiert, dass mehrere Anwender gleichzeitig mit ihr interagieren können. Damit eingegebene Daten dem richtigen Anwender zugeordnet werden können, wird von Webanwendungen jeder Zugriff in eine eigene Sitzung oder Session, die dem Anwender zugeordnet ist, sortiert. Es ist sofort ersichtlich, dass bei Übernahme der Session eines anderen Anwenders auch möglicherweise die Daten des anderen Anwenders übernommen werden können.

Wird beispielsweise die Session über eine Session-ID zugeordnet, die nur über einen URL-Parameter zwischen Webanwendung und Client ausgetauscht wird, so könnte ein Angreifer versuchen, durch Erraten anderer Session-IDs in andere Sessions einzudringen. Es sollte daher vom Prüfer beispielsweise geprüft werden, ob bei einer vorhandenen Zugriffskontrolle geprüft wird, ob eine Session von dem angemeldeten Anwender oder dem Client gesichtet werden darf.

Zugriffskontrolle

Wenn eine Webanwendung sensible Daten verarbeitet, so wird dies über eine Zugriffskontrolle gesteuert. In den meisten Fällen müssen sich die Anwender hierzu gegenüber der Anwendung authentisieren und ihrer Session werden die entsprechenden Zugriffsrechte eingeräumt, damit der Anwender die entsprechenden Daten oder Bereiche der Webanwendung sichten oder bearbeiten kann. Auch hier kann ein Angreifer durch das Erlangen der Zugriffsrechte eines anderen Anwenders großen Schaden anrichten. Es gibt verschiedene Möglichkeiten, eine Zugriffskontrolle umzusetzen. Hier muss je nach vorgefundener Methode geprüft werden, ob die erwarteten Sicherheitsvorkehrungen umgesetzt wurden. Benutzeranmeldung mit Benutzername und Passwort, Sicherheitsabfragen, Passwort-Vergessen-Funktionen oder verwendete Zertifikate können zahlreiche Schwächen enthalten, die ein Angreifer finden könnte und daher von dem Prüfer überprüft werden sollten.

Verschlüsselung

Neben der Zugriffskontrolle sollte eine Webanwendung darauf achten, dass sensible Daten nur verschlüsselt übertragen werden. Das HTTP-Protokoll beinhaltet, dass die Daten im Klartext übertragen werden und an jeder Netzwerkschnittstelle, auf die ein Angreifer Zugriff erhalten könnte, mitgelesen werden kann. Daher sollte alles, was nicht für die Allgemeinheit bestimmt ist, nur verschlüsselt übertragen werden. Aber auch wenn die Daten verschlüsselt übertragen werden, gibt es Schwachstellen, über die Angreifer Zugriff auf die Daten erhalten könnten. So müssen Webanwendungen beispielsweise damit rechnen, dass eine Vielzahl von unterschiedlichen Clients auf sie zugreift. Die meisten Webanwendungen bieten daher eine ebenso große Vielzahl von Möglichkeiten an, die Daten verschlüsselt zu übertragen. Die hierzu eingesetzten Cipher-Suiten

enthalten dabei auf der einen Seite sehr starke Algorithmen, die den aktuellen Empfehlungen entsprechen, auf der anderen Seite aber als schwächer eingestufte Algorithmen, die aus Kompatibilitätsgründen weiter verwendet werden. Die Prüfer sollten an dieser Stelle die unterstützen Algorithmen prüfen und auf entsprechende Empfehlungen hinweisen.

Fehlerhandling

Der Anwendungsprogrammierer möchte bei Eintritt eines Fehlers so viele Informationen wie möglich erhalten, um den Fehler schnell beseitigen zu können. Wenn diese Fehlermeldungen allerdings an unbekannte Anwender im Internet weitergegeben werden, können einige Informationen nützlich für einen potentiellen Angreifer sein. Er kann seine Angriffe beispielsweise besser planen, wenn er Softwareversionen, Datenbankbefehle oder Parameternamen kennt. Die Prüfer sollten daher die Anwendung so bedienen, dass möglichst viele Fehlerroutinen ausgelöst werden. Aus dem Verhalten der Anwendung und dahinter liegender Systeme kann dann auf weitere Angriffsmöglichkeiten geschlossen werden.

Absicherung der beteiligten Datenbanken und Anwendungen

Sobald Daten verarbeitet oder verwaltet werden, benötigen Webanwendungen weitere IT-Systeme im Hintergrund wie Datenbanken oder IT-Anwendungsserver für Dienste, die beispielsweise intensive Rechenaufgaben für die Webanwendung ausführen. Diese IT-Systeme sollten immer gut, von der Webanwendung selbst und damit einem möglichen Zugriff von außen, abgeschirmt sein. Der Prüfer sollte dies prüfen. Wenn erwartet wird, dass Daten beispielsweise an Datenbanken weitergegeben werden, so kann der Prüfer versuchen, Datenbankbefehle weiterzureichen.

Absicherung der Dateiuploadmöglichkeiten und weiterer spezieller Interaktionsmöglichkeiten

Der Dateiaustausch über eine Webanwendung stellt eine spezielle Anwendungsmöglichkeit dar, die gut abgesichert sein muss, damit ein Angreifer keine Schadprogramme an die Webanwendung übergeben kann. Daneben gibt es zahlreiche Interaktionsmöglichkeiten, die innerhalb von Webanwendungen umgesetzt und damit ausgenutzt werden können. So könnte beispielsweise der Mail-Versand von einer Seite-Empfehlen-Funktion als SPAM-Relais ausgenutzt werden kann.

Versteckte Parameter und Verzeichnisse

Die meisten Webanwendungen arbeiten mit einer Vielzahl von nicht direkt sichtbaren Parametern. Es gibt versteckte Felder, in denen Anwendungsentwickler Daten für den späteren Gebrauch ablegen oder nicht aktivierte Eingabefelder, die nur verwendet werden, wenn der Anwender bestimmte Zugriffsrechte besitzt. Manchmal wird an dieser Stelle die Absicherung vergessen, da die Felder ja nicht sichtbar sind oder nur von einem „vertrauenswürdigen“ Benutzerkreis verwendet werden. Auch hiernach sollte ein Prüfer Ausschau halten, ebenso nach nicht verlinkten Verzeichnissen. Bei Kenntnis der eingesetzten Anwendungen und Betriebssysteme kann auf die dahinterliegende Verzeichnisstruktur geschlossen werden. Es sollte überprüft werden, ob diese gut nach außen abgesichert ist und keine Testseiten oder Archivseiten zugreifbar sind, die nicht für den Anwender bestimmt sind. Auch der Zugriff auf das Icons-Verzeichnis kann einem möglichen Angreifer Informationen für seinen Angriff liefern, da er hier manchmal Rückschlüsse auf eingesetzte Anwendungen und teilweise sogar Versionen ziehen kann.

Modul 3 – Logische Fehler/Konfigurationsfehler

Die bislang beschriebenen Schwachstellen bezogen sich weitestgehend auf eine schlechte Absicherung. In der heutigen Zeit mangelt es auf Seiten der Anbieter aber oft an Ressourcen wie Zeit, Geld oder gut ausgebildetem Personal, so dass der Mensch als mögliche Schwachstelle hinzukommt. Gerade der Bereich Webanwendung entwickelt sich so schnell, dass die Techniker, die

den Webauftritt aufsetzen, nicht schnell genug alle neuen Funktionen lernen können. Die neuen Anwendungen sollen schnell über das Internet verfügbar gemacht werden. Wird ausreichend Zeit eingeplant, ist die eingesetzte Technik veraltet oder manchmal das Problem nicht mehr gefragt. Ausreichend Zeit wäre allerdings notwendig, um das komplexen Gebilde eines Webauftritts sauber zu konfigurieren. Oft wird im Betrieb mal schnell etwas verändert, zum Beispiel damit eine Funktion realisiert werden kann und es wird nicht überprüft, ob hierbei Seiteneffekte auf andere Funktionen eingetreten sind. Oder ein Administrator baut sich einen kurzen und einfachen Zugang ein, um etwas zu testen und vergisst den Zugang. Das sollte nicht passieren. Aber solche menschlichen Fehler sind gerade unter enormen Zeitdruck leider nicht vermeidbar. Auch hiernach sollte ein Prüfer suchen.

Auch innerhalb der Konfiguration des Webauftritts können zahlreiche Einstellungen genutzt werden, um Angriffe zu vermeiden. Das HTTP-Protokoll wurde nach dem bekannt werden von Angriffe weiterentwickelt. Es gibt eine Vielzahl von Einstellmöglichkeiten, die Angriffe erschweren. Beispielsweise können Cookies bei Bedarf mit den Attributen „HttpOnly“ und „secure“ versehen werden, um zu verhindern, dass sie über Skriptcode verändert oder trotz Verschlüsselung im Klartext übermittelt werden. Hier helfen dem Prüfer aber auch dem Webentwickler automatisierte Tools, solche Schwachstellen zu finden.

Optional: Modul 4 – Exploits

Der exakte Nachweis, dass eine Schwachstelle vorhanden ist, findet nur statt, wenn sie auch ausgenutzt wird, also ein Exploit erfolgreich eingesetzt wird. Dies ist allerdings mit Gefahren verbunden. Ein Exploit ist eine Befehlsfolge, um bekannte Sicherheitslücken auszunutzen. Dabei handelt es sich im Allgemeinen um Skripte, die von verschiedenen Quellen, häufig frei über das Internet, zur Verfügung gestellt werden. Ist der Exploit unsicher programmiert, so kann er Schaden an der IT-Anwendung anrichten. Im einfachsten Fall kann ein Absturz die Folge sein, es können aber auch Speicherbereiche überschrieben werden, die für das Funktionieren der IT-Anwendung oder des gesamten IT-Systems erforderlich sind und damit die IT-Anwendung oder das gesamte IT-System unbrauchbar machen. Hier muss genau abgewogen werden, ob ein Exploit eingesetzt wird.

> Das BSI empfiehlt, das Prüfer nur solche Exploits einsetzen, deren Wirkungsweise sie schon untersucht und getestet haben.

Abschlussgespräch

Nach Abschluss der Tests sollte ein Gespräch zwischen den Prüfern und den Ansprechpartnern seitens der Auftraggeber stattfinden. Ziel ist, über den Verlauf und die Ergebnisse der praktischen Prüfung zu informieren. Da der IS-Webcheck nicht vor Ort stattfindet, wird das Abschlussgespräch in der Regel telefonisch durchgeführt.

Wenn die Prüfer kritische Schwachstellen gefunden haben, sollten die Verantwortlichen vor Ort die Möglichkeit haben, diese sofort zu beseitigen. Hierzu ist es wichtig, dass die gefundenen kritischen Schwachstellen von den Prüfern ausreichend schnell ausgewertet werden.

> Um die Tests nicht unnötig zeitlich auszudehnen, wird *vom BSI empfohlen*, nicht alle Auswertungen direkt vorzunehmen. Daher kann die Vorstellung der Schwachstellen im

Abschlussgespräch unter Umständen nur unter Vorbehalt stattfinden. Eine verbindliche Darstellung aller gefundenen Schwachstellen sollte im Bericht zu finden sein.

4.3 Bericht

Das letzte Arbeitspaket eines IS-Webchecks stellt der Bericht dar. Der Bericht sollte wegen des möglicherweise brisanten Inhalts nur dem Prüfer persönlich, seiner Qualitätssicherung sowie einem ausgewählten Kreis des Auftraggebers zur Verfügung gestellt werden. Je nach Kritikalität müssen Vertraulichkeitskennzeichnungen des Dokumentes vorgenommen werden.

Zunächst sollte die Zielgruppe des Dokumentes seitens des Auftraggebers geklärt werden. Wenn das Management einen Bericht benötigt, so sollten keine technischen Einzelheiten vermerkt werden.

Anderseits benötigen Techniker genaue Beschreibungen der gefundenen Schwachstellen, damit sie diese nachvollziehen können. Es sollten auch Empfehlungen enthalten sein, welche Maßnahmen die Schwächen beseitigen. Hier sollte ein neutraler Prüfer Produktempfehlungen vermeiden. Es genügt, auf Klassen von Produkten hinzuweisen.

Das BSI empfiehlt, den Bericht mit der Beschreibung des Prüfobjekts und des Prüfmoduls zu starten. Anschließend sollte eine Managementzusammenfassung folgen, die dem Management vorgelegt werden kann und die Kernaussagen enthält. In weiteren Kapiteln werden dann die gefundenen Schwachstellen für die Techniker mit genauen Beschreibungen und Empfehlungen aufgelistet.

Im technischen Teil kann der Bericht nach Teilanwendungen strukturiert oder nach Kritikalität der gefundenen Schwachstelle gruppiert werden.

Für die Bewertung der Schwachstellen können verbreitete Industriestandards wie CVSSv2 [13] oder DREAD [14] von Microsoft herangezogen werden.

Die Einstufung der gefundenen Schwachstellen bzgl. der Kritikalität erleichtert es den Administratoren, eine Reihenfolge bei der Behebung der Schwachstellen einzuplanen.

Das BSI bewertet bei IS-Penetrationstests die gefundenen Schwachstellen bezüglich der Kritikalität wie folgt:

Schadenspotenzial	Erforderliche Reaktion	Erläuterung
hoch	sofort	Fremdsteuerung des Prüfobjekts durch Angreifer möglich, Verlust von sensiblen Daten möglich, Veränderung des Prüfobjekts oder Auslesen von sensiblen Daten durch

Schadenspotenzial	Erforderliche Reaktion	Erläuterung
		Angreifer möglich
mittel	kurzfristig	Schwachstellen, die schwerwiegende Angriffe ermöglichen können
niedrig	mittelfristig	Schwachstellen, die ein unbestimmtes Angriffspotenzial haben
zur Information	langfristig	Verbesserungspotenzial

Die Einstufung der gefundenen Schwachstellen hängt dabei jeweils vom Sicherheitsbedarf der verarbeiteten Daten ab. Dieselbe Schwachstelle wird unterschiedlich eingestuft, abhängig davon ob offene oder geschützte Daten verarbeitet werden.

Ebenso fließt in die Einstufung der gefundenen Schwachstellen eine Einschätzung der Wahrscheinlichkeit ein, dass der Angriff durchgeführt wird. Diese wird anhand der benötigten Fähigkeiten und Mittel abgeschätzt, einen Angriff durchzuführen.

Die Erfahrung zeigt, dass zu ausführliche Berichte nicht ausreichend genug gelesen werden. Es empfiehlt sich daher, Gruppierungen von gefundenen Schwachstellen vorzunehmen. Beispielsweise könnte bei 100 Formularseiten derselbe Fehler vorliegen. Wenn der Fehler 100 Mal exakt gleich im Bericht beschrieben wird, so könnten die Administratoren den Einstiegspunkt für den nächsten relevanten Fehler überblättern.

Es wird empfohlen, eine Schwachstellenbeschreibung einmal vorzunehmen, hierzu ein Beispiel genau auszuführen und darauf hinzuweisen, dass alle gleich aufgebauten Seiten, ebenfalls diesbezüglich geändert werden müssen.

5 Anhang

5.1 Checklisten

5.1.1 Hilfestellung für die Beauftragung von IS-Webchecks

Eine Leistungsbeschreibung zur Beauftragung von IS-Webchecks sollte neben den beschaffungsrelevanten Vorgaben folgende technische Aspekte enthalten:

Vorgabe	**Spezifizierung**	**Bemerkung Institution (erledigt oder nicht relevant, weil...)**
Motivation für IS-Webcheck (Kapitel 2.1.1)	Check der Sicherheitsmaßnahmen, Verdacht auf Angriff, entdeckter Angriff	
Anforderung an Prüfer (Kapitel 2.2)	Fachliche Anforderungen	
	Weitere Fähigkeiten	
	Arbeitet für Prüfstelle	
	Technische Qualifikation / Zertifikate	
Rahmenbedingungen (Kapitel 2.3)	Vertrag, NDA, Speicherzeiten von Daten	
	Datenschutz, Geheimschutz, Personalvertretung	
	Sonstiges (Wartungsarbeiten)	
Festlegung des Prüfobjekts zwischen Prüfer und Institution (Kapitel 3.1	URL/IP-Adresse Zugangsdaten zu geschützten Bereichen	
Festlegung des Prüfumfangs (Kapitel 3.2)	Prüftiefe	
	Prüfort	
	Prüfzeitraum	
	Prüfbedingungen	
Verantwortlichkeiten (Kapitel 3.1.4)	Projektverantwortliche bei Prüfern und Institution	
Meilensteinplan (Vgl. auch	Einarbeitungsphase	

Vorgabe	Spezifizierung	Bemerkung Institution (erledigt oder nicht relevant, weil...)
Mindestanforderungen IS-Webcheck Kapitel 5.1.2)	Testphase	
	Berichtsphase	

5.1.2 Mindestanforderungen an einen IS-Webcheck

Diese Checkliste soll helfen die organisatorischen und fachlichen Rahmenbedingungen, die bei einem IS-Penetrationstest erfüllt werden müssen, strukturiert durchzuführen. Darüber hinaus sind in der Checkliste die wiederkehrenden Elemente eines IS-Penetrationstests aufgenommen.

Sollten einzelne Pakete nicht bearbeitet werden, so sollte der Grund dafür nachvollziehbar sein. Beispielsweise müssen die Kunden/Mitarbeiter nicht zwingend informiert werden, wenn durch die Tests keine Beeinträchtigung zu erwarten sind.

Arbeitspaket	Unterpaket 1	Unterpaket 2	Unterpaket 3	Erforderliche Personen	Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)
Einarbeitung Prüfer (Kapitel 4.1)	Dokumente sichten			Prüfer	
Vorbereitung Institution	Prüfumgebung bereitstellen (Kapitel 3.2 Prüfumfang)			Ansprechpartner Institution /Hoster (Administrator, Techniker)	
	Kunden/Mitarbeiter informieren (Kapitel 2.3 Rahmenbedingungen)			Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
	Datenschutzbeauftragten/Personalrat/Geheimschutzbe auftragten einbeziehen (Kapitel 2.3 Rahmenbedingungen)			Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
	Dokumente an Prüfer schicken (Kapitel 4.1)			Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
Test des Prüfobjekts (Kapitel 4.2)	Anfangsgespräch			Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-	

Arbeitspaket	Unterpaket 1	Unterpaket 2	Unterpaket 3	Erforderliche Personen	Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)
				wortlicher oder Fachverantwortliche)	
	Prüfumgebung			Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant wortlicher oder Fachverantwortliche)	
	Praktische Prüfung	Modul 1 – Schwachstellensuche		Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
		Modul 2 – Schwach-stellentest	Eingabevalidierung	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
			Session Handling	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
			Zugriffskontrolle	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant wortlicher oder Fachverantwortliche)	
			Verschlüsselung	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
			Fehlerhandling	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	

Arbeitspaket	**Unterpaket 1**	**Unterpaket 2**	**Unterpaket 3**	**Erforderliche Personen**	**Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)**
			Absicherung der beteiligten Datenbanken und Anwendungen	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
			Absicherung von Dateiuploadmöglichkeiten und weiteren Interaktions-möglichkeiten	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
			versteckte Parameter/ Verzeichnisse	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
		Modul 3 – logische Fehler/Konfigurationsfehler		Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
		Optional: Modul 4 – Exploits		Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
	Abschlussgespräch			Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
Bericht (Kapitel 4.3)		Einleitung		Prüfer	
		Managementzusammenfassung			
		Technische Beschreibung der Schwachstellen mit Empfehlungen und Einstufung der Kritikalität			

5.2 Ablaufplan

Dieser Ablaufplan soll helfen die organisatorischen und fachlichen Rahmenbedingungen, die bei einem IS-Weebcheck erfüllt werden müssen, strukturiert darzustellen. Es sind die wiederkehrenden Elemente eines IS-Webchecks aufgenommen. Je nach Prüfobjekt müssen einzelne Aspekte angepasst und erweitert werden.

Sollten einzelne Pakete nicht bearbeitet werden, so sollte der Grund dafür nachvollziehbar sein. Beispielsweise müssen die Kunden/Mitarbeiter nicht zwingend informiert werden, wenn durch die Tests keine Beeinträchtigung zu erwarten sind.

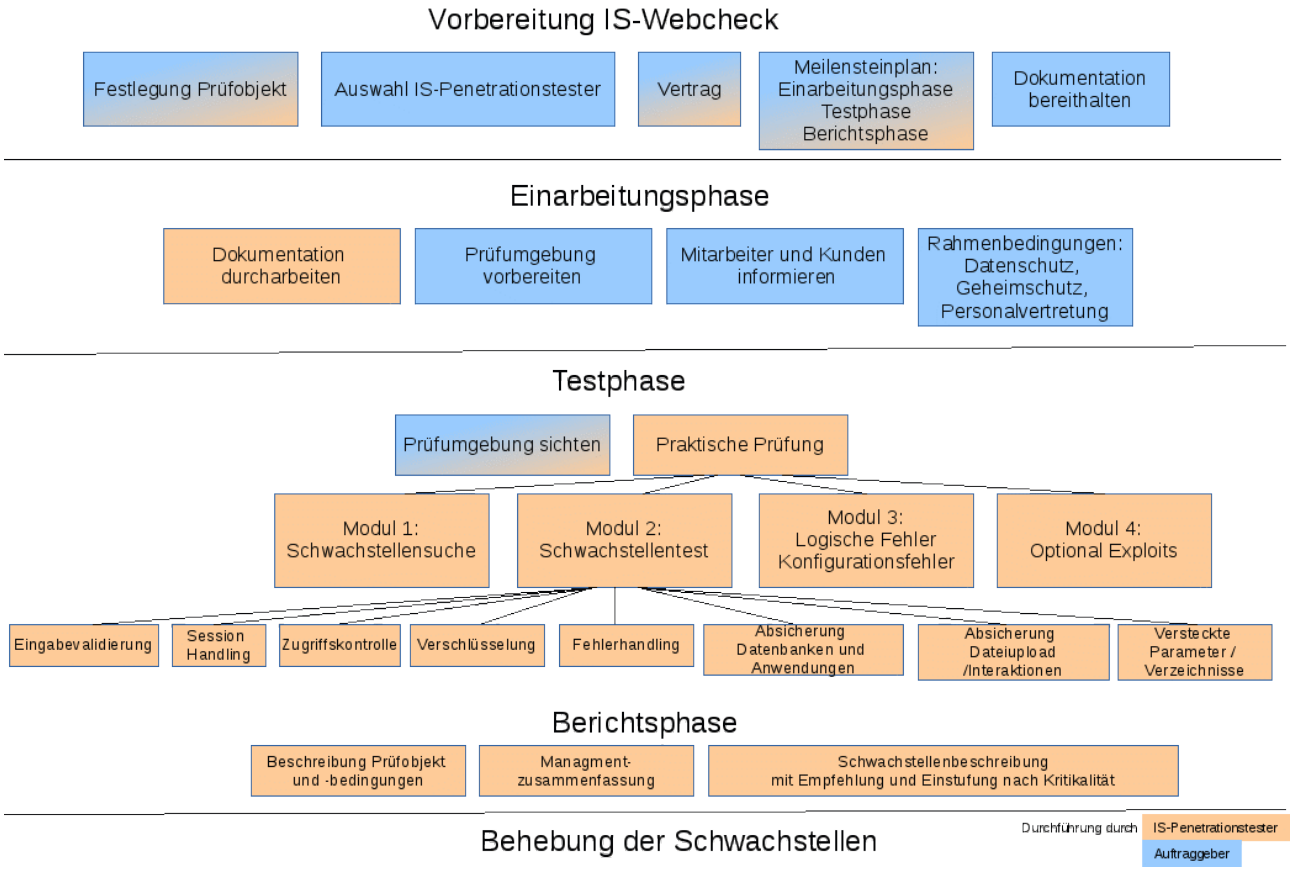


Abbildung 3 Ablauf eines IS-Webcheck

6 Glossar

Das Glossar beinhaltet einige der im Leitfaden verwendeten Begriffe sowie einige gängige Begriffe aus dem IS-Penetrationstest/IS-Webcheck-Bereich. Die Autoren haben eine kleine Auswahl getroffen, die bei Weitem nicht vollständig ist. Weitere Begriffe können im Internet nachgeschlagen werden.

Begriff	Erläuterung
APT	Ein Advanced Persistent Threat (APT) ist ein sehr komplexer, zielgerichtet durchgeführter Cyber-Angriff
Buffer Overflow	Es werden Daten in einen Speicherbereich geschrieben, der kleiner als die geschriebene Datenmenge ist. Wenn das Programm dies nicht abfängt, wird der Speicher hinter dem reservierten Speicherbereich überschrieben. Bei Kenntnis der Nutzung des Speicherinhalts können hierdurch gezielte Angriffe durchgeführt werden.
Cross-Site Scripting Angriff	Bei Cross-Site Scripting-Angriffen (XSS-Angriffen) versucht ein Angreifer indirekt Schadcode (in der Regel Browser-seitig ausführbare Skripte, wie JavaScript) an den Client des Benutzers der Webanwendung zu senden. Werden die Ein- und Ausgaben von einer Webanwendung nicht ausreichend validiert, so kann ein Angreifer schadhaften Code in die Webanwendung einschleusen (z. B. innerhalb eines Kommentars zu einem Artikel) und so verteilen. Wird eine infizierte Webseite von einem Benutzer aufgerufen, führt der Client (z. B. Browser) den eingefügten Schadcode aus. Aus Sicht des Benutzers stammt der schadhafte Code von der Webanwendung und wird somit als vertrauenswürdig eingestuft. Daher wird der Schadcode im Sicherheitskontext der Webanwendung interpretiert und es ist dem Angreifer möglich, Befehle im Kontext einer möglicherweise bestehenden Sitzung des betroffenen Benutzers auszuführen. Es gibt drei Arten von XSS-AngriffenAttacken: non-persistent, persistent und DOM-based.

Begriff	Erläuterung
DoS	Bei einem Denial of Service (DoS)-Angriff werden so viele Anfragen an einen Dienst gleichzeitig ausgeführt, dass er (kurzfristig) ausfällt. Wenn die Anfragen von verschiedenen IP-Adressen ausgeführt werden, so wird auch von einem distributed Denial of Service (dDoS) gesprochen.
Exploit	Ein Exploit ist ein Programm, dass eigens zum Ausnutzen einer Sicherheitslücke geschrieben wurde.
IS-Penetrationstest	Bei IS-Penetrationstests werden vorrangig Schnittstellen nach außen untersucht, über die potenzielle Angreifer in die untersuchten IT-Systeme eindringen könnten. Hierbei werden Konfigurationsfehler sowie noch nicht behobene Schwachstellen identifiziert.
IS-Revision	Die IS-Revision zielt darauf ab, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und der Sicherheitsprozesse zu optimieren.
IS-Webcheck	Mit einem IS-Webcheck wird der Sicherheitsstand einer Internetpräsenz geprüft. Hierbei werden Tests auf die Webanwendung größtenteils durch den Einsatz automatisierter Methoden über das Internet durchgeführt.
Passiver Schwachstellenscan	Ein Prüfer scannt mit eigenen Geräten im Zielnetz nach bekannten Schwachstellen. Er setzt hierzu Schwachstellenscanner ein, nutzt die Schwachstellen aber nicht aus.
Portscan	Ein Prüfer scannt in einem Netzwerk oder Netzsegment nach offenen Ports.
Prüfobjekt	Das Prüfobjekt grenzt ab, welches IT-System getestet wird. Hierbei wird aus Angreifersicht geschaut, wo Schnittstellen auf die IT-Systeme sind, über die ein Angreifer eindringen kann. Übliche Prüfobjekte sind u.a. • Netzkoppelelemente (Router, Switches,

Begriff	Erläuterung
	Gateways) • Sicherheitsgateways (Firewalls, Paketfilter, Intrusion Detection System, Virenscanner, etc.) • Server (Datenbankserver, Webserver, Fileserver, Speichersysteme, etc.) • Telekommunikationsanlagen • Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop) • Clients • Drahtlose Netze (WLAN , Bluetooth) • Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)
Prüftiefe	Es wird festgelegt, in welcher Tiefe ein Test durchgeführt werden soll. Hierbei kann beispielsweise ein Sichereitsaudit, ein nicht invasiver Schwachstellenscan oder das Einsetzen von Exploits (aktiver Schwachstellenscan) zur Auswahl stehen.
Prüfumfang	Der Prüfumfang definiert die Prüftiefe (technisches Sicherheitsaudit, nicht invasiver Schwachstellenscan oder Einsetzen von Exploits), den Prüfort (Institution Rechenzentrum, Institution Büroräume oder vom dem Prüflabor aus über das Internet), den Prüfzeitraum und die Einrichtung der Prüfumgebung (Freischaltung von MAC-Adressen für Laptops von Prüfern, Freischalten des Sicherheitsgateways für die Prüfer).
Session	Webanwendungen sind im Regelfall so konzipiert, dass mehrere Anwender gleichzeitig mit ihr interagieren können. Damit eingegebene Daten dem richtigen Anwender zugeordnet werden können, wird von Webanwendungen jeder Zugriff in eine eigene Sitzung oder Session, die dem Anwender zugeordnet ist, sortiert.
Social Engineering	Bei Social Engineering Angriffen werden über

Begriff	Erläuterung
	die Gutgläubigkeit der Mitarbeiter/Zielpersonen, aber auch über Informationen, die im Internet (beispielsweise Social Media oder Foren) frei verfügbar sind, Kenntnisse über die Strukturen einer Institution und auch über deren IT-Systeme zusammengetragen, um bei weiteren Angriffen gezielt darauf aufbauen zu können.
Spoofing	Spoofing steht für das Vortäuschen einer falschen Identität. Beispielsweise können die MAC-Adresse, die IP-Adresse oder die Absenderadresse bei E-Mails relativ leicht gefälscht werden. Wird dies gemacht, wird von Spoofing-Angriffen gesprochen.
SQL-Injection Angriff	SQL-Injection bezeichnet das Einschleusen schädlicher oder unerwünschter Datenbankbefehle in die Datenbankabfragen einer Anwendung. Ermöglicht wird diese Technik durch eine unzureichende Prüfung der Eingaben innerhalb der Anwendung. Dadurch ist es möglich, eigene Befehle an die Datenbank zu senden, wodurch unberechtigt Daten gelesen, bzw. verändert werden können oder die vollständige Kontrolle über den Server erlangt werden kann.
Technisches Sicherheitsaudit	Bei einem technischen Sicherheitsaudit wird anhand der Versionen der eingesetzten IT-Anwendungen auf mögliche Schwachstellen geschlossen. Die Prüfer bedienen die IT-Systeme hierbei nicht selbst, sondern lassen sich von einem Administrator zeigen, welche Versionen eingesetzt und welche Härtungsmaßnahmen durchgeführt wurden.

7 Referenzen

Trotz sorgfältiger Prüfung kann das BSI für die hier verlinkten Inhalte keine Haftung übernehmen.

[1] Leitfaden IS-Revision
https://www.bsi.bund.de/dok/6621784

[2] IT-Grundschutz
https://www.bsi.bund.de/dok/6604654

[3] IS-Penetrationstest/IS-Penetrationstest des BSI
https://www.bsi.bund.de/dok/6621966

[4] Personenzertifizierung des BSI
https://www.bsi.bund.de/dok/6617744

[5] Council for Registered Ethical Security Testers (CREST)-Zertifizierung (UK, Australia)
http://www.crest-approved.org/
http://www.crestaustralia.org/approved.html

[6] Certified Ethical Hacker (CEH)-Zertifizierung (USA)
http://www.eccouncil.org/Certification/certified-ethical-hacker

[7] Leitfaden IS-Penetrationstest

https://www.bsi.bund.de/dok/6621966

[8] Sicheres Bereitstellen von Web-Angeboten (Isi-Web-Server)
https://www.bsi.bund.de/dok/6620604

[9] BSI-Leitfäden zur Entwicklung sicherer Webanwendungen
https://www.bsi.bund.de/dok/6624588

[10] Sicherheit von Webanwendungen: Maßnahmenkatalog und Best Practices
https://www.bsi.bund.de/dok/6624424

[11] The Web Application Hackers Handbook 2 (Dafydd Stuttard, Marcus Pinto)
http://mdsec.net/wahh/

[12] The OWASP Testing Checklist
https://www.owasp.org/index.php/Testing_Checklist

[13] NVD Common Vulnerability Scoring System Support v2 (CVSSv2)

https://www.first.org/cvss

[14] Microsoft Thread Modeling (Einstufung mit DREAD)

http://msdn.microsoft.com/en-us/library/ff648644.aspx