Bundesamt
für Sicherheit in der
Informationstechnik

Ein Praxis-Leitfaden für den IS-Webcheck

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 1.6 (31.1.2020)

Inhalt

1 Einleitung

Im Folgenden wird der IT-Sicherheits-Webcheck oder kurz IS-Webcheck als eine spezielle Variante des IS-Penetrationstests [6] 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 kostensparenden 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 einsetzen möchten, 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.

- Der regelmäßige IS-Webcheck zur Überprüfung des Sicherheitsstands der Webanwendung sollte als Teil des ISMS-Prozess eingesetzt werden. [1]
- Als Sicherheitsüberprüfung kritischer Infrastrukturen (KRITIS) wird der IS-Webcheck im Rahmen des BSI Gesetzes gefordert. [2]
- Für kritische Geschäftsprozesse ist die Durchführung eines IS-Webchecks im Rahmen des Umsetzungsplans Bund vor Inbetriebnahme der Geschäftsprozesse vorgegeben.[3] [4]

Der IS-Webcheck ist auch ein Instrument um den Sicherheitsstandard genutzter Webanwendungen zu bestimmen, um Mängel zu beseitigen und diese vor möglichen Angriffen zu schützen.

[1] siehe auch: “Auswahl von Sicherheitsmaßnahmen [DOK]“ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node.html

[2] siehe auch: “ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“ https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html/

[3] siehe auch: “5.2 Ressort- und einrichtungsinterne Maßnahmen“ https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html/

[4] siehe auch: “3.3 Anforderungen bei erhöhtem Schutzbedarf“ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_1_Webanwendungen.html

1.1.1 Integration in den ISMS-Prozess

Die Praxis zeigt, dass eine umfassende, unternehmens- bzw. behördenweite Informationssicherheit, die auf dauerhafte Erfüllung der Anforderungen und nachhaltige Begrenzung der Risiken ausgerichtet ist, nur durch ein Informationssicherheitsmanagement erreicht werden kann. Der BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)“ (siehe [13]) beschreibt den Informationssicherheitsprozess. Innerhalb des ISMS kann der IS-Webcheck als Teil des Informationssicherheitsprozesses genutzt werden und fügt sich in die „Check“-Phase nach dem PDCA-Modell von Deming ein.

Der Informationssicherheitsprozess wird von der Leitungsebene initiiert und beginnt mit der „Plan“-Phase. In dieser Phase wird die Sicherheitsorganisation aufgebaut.

In der anschließenden „Do“-Phase werden das Sicherheitskonzept erstellt und die erforderlichen Maßnahmen umgesetzt.

Die folgende „Check“-Phase dient der Überprüfung der IT-Sicherheitsstrategie, der IT-Sicherheitsorganisation, des Sicherheitskonzepts und der Umsetzung der IT-Grundschutz-Anforderungen der eingesetzten Webanwendung. Eine mögliche Methode der Erfolgskontrolle ist der IS-Penetrationstest und speziell der IS-Webcheck .

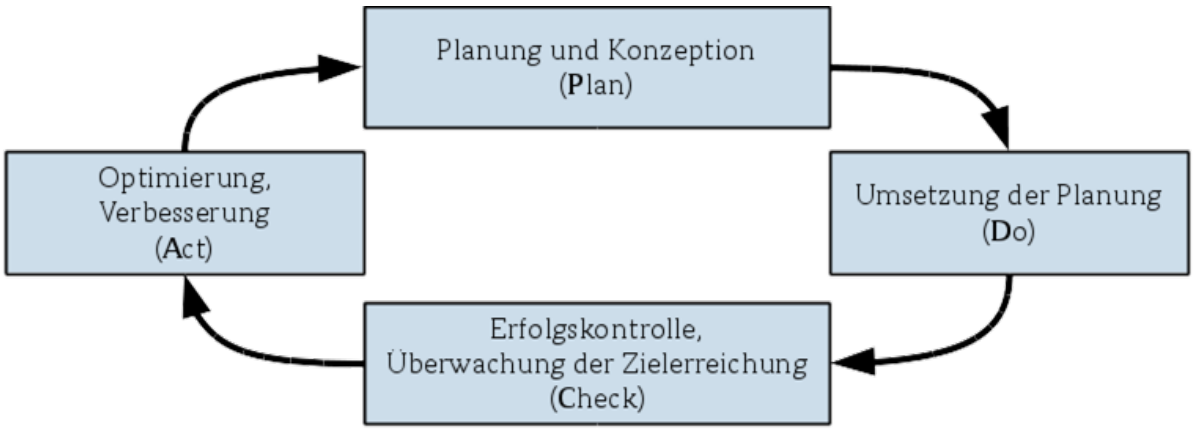

Abbildung 1: PDCA-Modell nach Deming

Das Ergebnis der „Check“-Phase, z. B. der Bericht des IS-Webchecks, wird gemäß dem Informationssicherheitsprozess in der darauf folgenden „Act“-Phase ausgewertet und weiterverarbeitet. Das bedeutet, dass die Geschäftsprozesse optimiert und Sicherheitslücken bei der Umsetzung der IT-Grundschutz-Anforderungen geschlossen werden.

Falls sich durch die Ergebnisse der „Check“-Phase grundlegende oder umfangreiche Veränderungen ergeben, so beginnt der Informationssicherheitsprozess vorzeitig wieder mit der „Plan“-Phase (siehe [13]). Der Kreislauf der IT-Grundschutz Vorgehensweise mit den prozessbeeinflussenden Ein- und Ausgabedokumenten wird im folgenden Diagramm dargestellt.

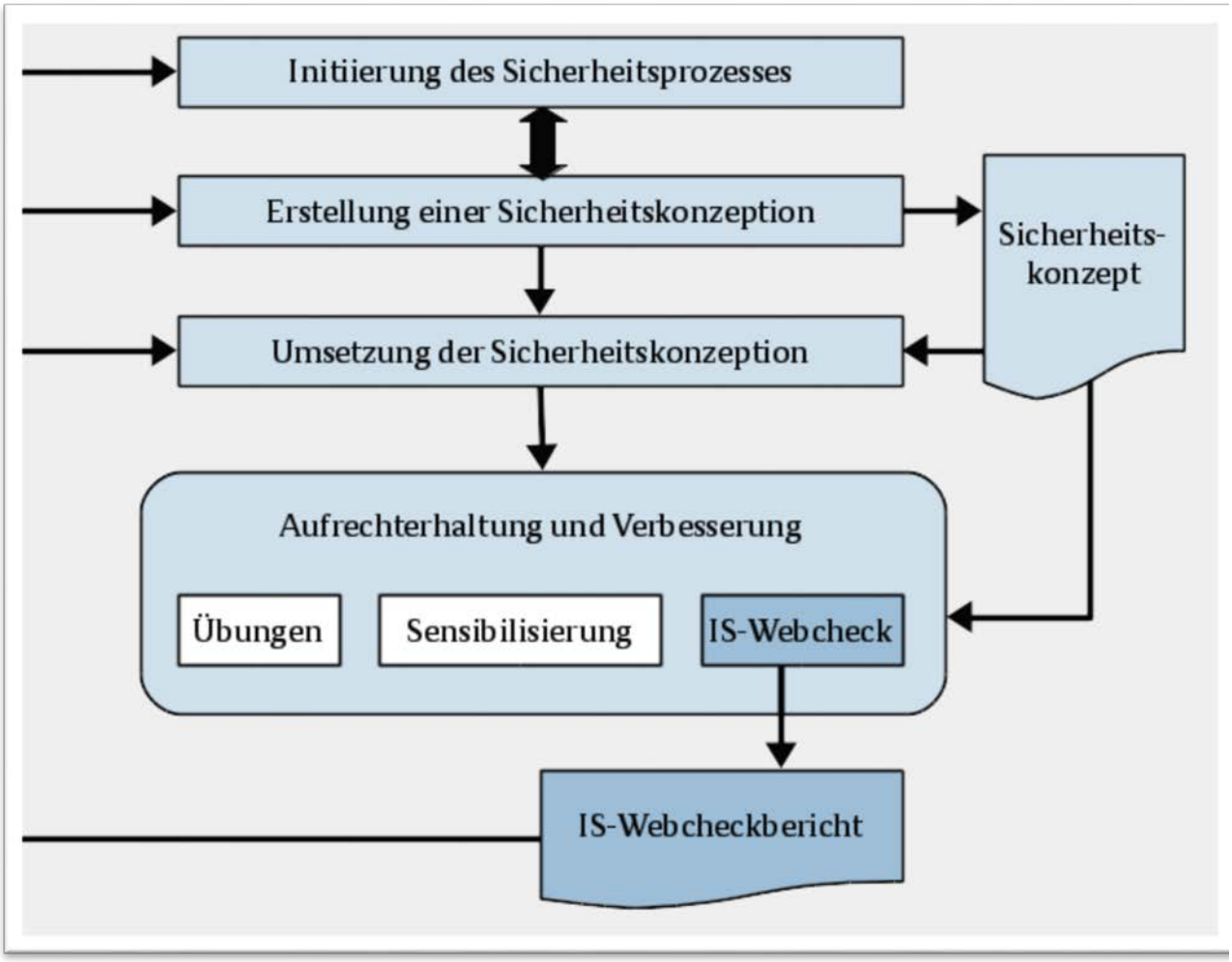

Abbildung 2: Einbettung des IS-Webchecks in das ISMS

1.2 Vorgaben für Bundesbehörden

Zur Evaluierung der Informationssicherheit wird auf Bundesebene jährlich eine Erhebung des Sachstands zur Umsetzung des UP Bund 2017 durchgeführt. Auf Ebene der Ressorts werden dazu die Maßnahmen des UP Bund 2017 auf Zielorientierung sowie Effektivität hin evaluiert. Informationssicherheitsmaßnahmen in den Einrichtungen müssen regelmäßig daraufhin überprüft werden, in wieweit sie die Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten Informationen gewährleisten. Auf Ebene der Einrichtungen sind daher in angemessenen Abständen entsprechende Audits, Reifegradprüfungen, IS-Revisionen und IS-Penetrationstests durchzuführen. Die Ergebnisse von Überprüfungen und Tests sowie die daraufhin eingeleiteten Maßnahmen sind in der Informationssicherheitsdokumentation festzuhalten. „Besonderer Sorgfalt bedarf es vor der Inbetriebnahme neuer, direkt an das Internet angebundener Fachanwendungen. Dazu sind geeignete Maßnahmen (z. B. WebCheck, Penetrationstest) vor Inbetriebnahme durchzuführen und zu dokumentieren. Die Maßnahmen sind wahlweise vom BSI oder von einem BSI zertifizierten Dienstleistungsunternehmen durchzuführen. Sofern das nicht möglich ist, kann ein anderes qualifiziertes und vertrauenswürdiges Dienstleistungsunternehmen beauftragt werden. Hierzu kann die Beratung durch das BSI in Anspruch genommen werden. Wesentliche Mängel sind vor einer Inbetriebnahme zu beseitigen. Die / der zuständige IT-SiBe ist zu beteiligen.“[5]

1.2.1 Vorgaben für Betreiber kritischer Infrastrukturen (KRITIS)

Die Vorgaben des IT-Sicherheitsgesetzes erfordern die Zusammenarbeit zwischen der betroffenen Industrie und dem BSI. Diese Zusammenarbeit wird auch in der Erweiterung des BSI-Gesetzes deutlich. Damit wird die Notwendigkeit der Sicherheitsüberprüfung von Webanwendungen ersichtlich. Als Standard für die Sicherheitsüberprüfungen der Webanwendungen kann ein IS-Webcheck eingesetzt werden.

Der Betreiber von kritischen Infrastrukturen soll alle zwei Jahre einen Nachweis in Form von Sicherheitsaudits, Prüfungen und Zertifizierungen vorlegen. Es ist empfehlenswert, als geeignete Prüfung der Sicherheit einer Webanwendung den IS-Webcheck im gleichen Zeitabstand (alle zwei Jahre) durchzuführen.

Aus dem aktuellen BSIG Version 2017 §8a (3) kann die Notwendigkeit eines regelmäßigen IS-Webchecks einer Webanwendung im Bereich KRITIS abgeleitet werden.[6]

1.2.2 Der Einsatz kritischer Geschäftsprozesse benötigt zusätzliche Sicherheitsmaßnahmen

Die Sicherheit kritischer Geschäftprozesse ist für den Betrieb und die Aufrechterhaltung der Arbeitsfähigkeit der Bundesverwaltung notwendig und erfordert verstärkte, vorrangige Sicherheitsmaßnahmen. Diese Sicherheitsmaßnahmen für Webanwendungen werden beim Betrieb und der Inbetriebnahme durch IS-Webchecks überprüft.

---

[5] siehe auch: Umsetzungsplan Bund (5.2) von 2017 „Ressort- und einrichtungsinterne Maßnahmen“ https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

[6] siehe auch: “Orientierungshilfe zu Nachweisen gemäß §8a (3) BSIG“ https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Nachweise/Orientierungshilfe/Orientierungshilfe_node.html

„Sicherheitskonzepte, die kritische Geschäftsprozesse berühren, sind durch die / den IT-SiBe im Rahmen des Informationssicherheitsprozesses prioritär zu behandeln. Kritische Geschäftsprozesse sind solche, die für die Aufgabenerfüllung und Zielerreichung sowie zur Aufrechterhaltung des Geschäfts- bzw. Dienstbetriebs einer Einrichtung und für die Arbeitsfähigkeit der Bundesverwaltung, eines Ressorts oder einer Einrichtung von essentieller Bedeutung sind.

Für kritische Geschäftsprozesse sind daher im Rahmen des Notfallmanagements insbesondere Maßnahmen zur Sicherstellung der Arbeitsfähigkeit (Business Continuity) unter Anwendung der einschlägigen BSI-Standards zu treffen.“[7]

Kritische Geschäftsprozesse weisen in der Regel einen höheren Schutzbedarf auf. Speziell für die Absicherung von IT-Systemen und IT-Verfahren kritischer Geschäftsprozesse sind erhöhte Anforderungen insbesondere im Hinblick auf die Verfügbarkeit, aber ggf. auch im Hinblick auf die Vertraulichkeit und / oder die Integrität zu erfüllen.

1.3 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 „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...

1.4 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.

[7] siehe auch: Umsetzungsplan Bund (6) von 2017 „Kritische Geschäftsprozesse“ https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

Eine Webanwendung ist nach der hier verwendeten Definition Teil eines Webauftritts. Dieser besteht aus (ggf. mehreren) Webanwendungen, die auf einem Webserver / Cluster installiert sind und mit anderen Anwendungen oder Datenbanken kommunizieren und über eine Netzwerkschnittstelle für Anwender über das Internet erreichbar sind. Ein Webauftritt ist darüber hinaus meistens durch ein Sicherheitsgateway geschützt (Siehe auch Abb. 3).

Das BSI empfiehlt, in verschiedenen Veröffentlichungen ([7], [8], [9]) 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 und Ausgabekodierung 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 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 Anwendungen hinter der Webanwendung vom Anwender direkt angesprochen werden können.

Auch eine mangelnde Eingabevalidierung und Ausgabekodierung 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.

Der IS-Webcheck erfolgt in Absprache mit dem jeweiligen Auftraggeber. Der Zugriff auf die zu testenden Webserver, Webapplikationsserver oder den zu testenden Webservice erfolgt daher in Absprache mit dem Hoster der Webseite(n). Diese Dienste sind von modernen Sicherheitsgateways vor dem nicht autorisierten Zugriff geschützt. Dagegen verfügt der Prüfer über umfangreiche Informationen über die zu testenden Systeme. Dazu gehören Informationen über das eingesetzte Content-Management-System (CMS), eingesetzte Betriebssysteme, Datenbanken und weitere Hilfsanwendungen.

Im Bereich der Webanwendungen existiert 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.

1.5 Abgrenzungen

1.5.1 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 es eine Checkliste für Prüfer, die abgearbeitet werden kann.

Auch Angreifer arbeiten nicht nach Checklisten, sondern 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.

1.5.2 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 auch, 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 (wie 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.

1.5.3 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.

ISO 27001 Audit

Die ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz geben Institutionen die Möglichkeit, ihre Bemühungen um Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen zu dokumentieren. Ziel dieser Zertifizierung ist es, die Erreichung der Sicherheitsziele der Institution und die Korrektheit und Vollständigkeit der Umsetzung der Sicherheitsanforderungen zu prüfen, zu bewerten und zu dokumentieren.

Werden im definierten Auditierungsschema Forderungen hinsichtlich Anzahl oder Umfang von durchzuführenden Prüfungen vorgegeben, so sind dies Mindestanforderungen. Dem Auditor ist es freigestellt, den Umfang der Prüfungshandlungen zu erweitern.

Als Ergebnis eines ISO27001 Audit steht eine K.O.-Prüfung zur Erteilung des Zertifikats.

IS-Kurzrevision

Die IS-Kurzrevision ist ein Verfahren zur Einschätzung des Informationssicherheitsstatus und -prozesses in einer Institution. Ziel der IS-Kurzrevision ist es, der Leitungsebene mit wenig Aufwand einen Überblick über den Sicherheitsstatus und die bestehenden sicherheitskritischen Themenbereiche in der eigenen Institution zu verschaffen.

Bei einer IS-Kurzrevision werden Anforderungen aus dem IT-Grundschutz betrachtet, die eine wesentliche Grundlage für Informationssicherheit bilden und sich darüber hinaus aufgrund von Erfahrungswerten als problembehaftet erwiesen haben.

Als Ergebnis der IS-Kurzrevision wird ein Mängelbericht zur Optimierung des Sicherheitsniveaus erstellt und dem Auftraggeber überreicht.

IS-Webcheck

Mit einem IS-Webcheck des BSI wird der Sicherheitsstand der Internetpräsenz einer Behörde oder einer Institution geprüft. Hierbei werden die Tests größtenteils durch den Einsatz automatisierter Methoden über das Internet durchgeführt.

Als Ergebnis des IS-Webchecks wird ein Mängelbericht mit Maßnahmenempfehlungen zur Optimierung des Sicherheitsniveaus erstellt und dem Auftraggeber überreicht.

IS-Penetrationstest

Bei einem 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. Bei einem IS-Penetrationstest durch das BSI kann in unterschiedlicher Prüftiefe getestet werden. Wenn ein vollständiger Sicherheitsstatus für einen Webauftritt erwünscht ist, wird empfohlen, einen IS-Penetrationstest zusätzlich zu dem IS-Webcheck durchzuführen.

Als Ergebnis eines IS-Penetrationstests wird ein Mängelbericht mit Maßnahmenempfehlungen zur Optimierung des Sicherheitsniveaus erstellt und dem Auftraggeber überreicht.

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

Im Rahmen des Code Review wird der Quellcode von Software systematisch untersucht. Dieser kann auch gezielt eingesetzt werden, um gängige Sicherheitslücken zu finden. Bei der Entwicklung von Systemen sollten Code Reviews stattfinden, da es hardwareabhängige Fehler gibt, die nur so mit vertretbarem Aufwand gefunden werden können. Der Aufwand dafür sollte sich am Schutzbedarf und am Kosten-Nutzen-Verhältnis orientieren. Bei höheren Sicherheitsanforderungen sollte eine formale Code-

Inspektion durchgeführt werden. Reviews senken die Kosten und bringen oft nur einen vertretbaren Sicherheitsverlust mit sich.[8]

- Können Feld-Indizes überlaufen?
- Sind alle Variablen im richtigen Kontext definiert?
- Ist die Bit-Breite der Variablen ausreichend?
- Werden arithmetische Überläufe erkannt und behandelt?
- Werden bekannte fehlerträchtige Konstrukte vermieden?

[8] siehe auch: „Leitfaden zur Entwicklung sicherer Webanwendungen“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftragnehmer.pdf?__blob=publicationFile&v=2

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 gibt 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 eine regelmäßige Überprüfung der getroffenen Schutzmaßnahmen durch IS-Webchecks nachdenken. Nicht nur ein Datenverlust kann brisant sein, sondern auch der Imageschaden bei einem erfolgreichen Angriff.

Ebenso besitzen Unternehmen Know-How, wie Fachkenntnisse und Patente, auf dem der wirtschaftliche Erfolg des Unternehmens beruht. Auch hier kann ein Angriff fatale wirtschaftliche 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.

Ein Sicherheitstest mit eingebundenem IS-Webcheck wird hier exemplarisch an der Vorgehensweise eines Sicherheitstests einer Behörde dargestellt. Die Vorgehensweise einer Institution mit anderer Organistionstruktur wird ähnlich durchgeführt.

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.

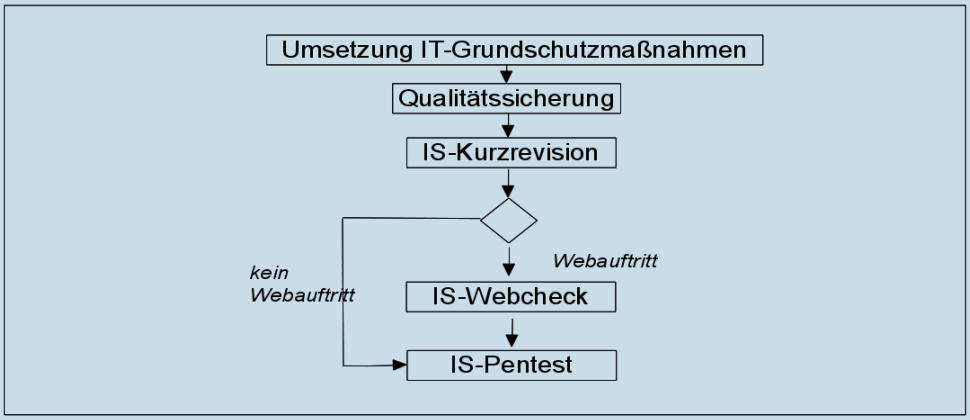

Abbildung 4: Reihenfolge der Sicherheitsmaßnahmen

2.1.3 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.

2.1.4 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.[9]

Die Unternehmen aus dem Bereich der kritischen Infrastrukturen (KRITIS) sind in verschiedene Sektoren aufgeteilt. Diese werden im BSI Gesetz §2 definiert.[10] Webanwendungen von Unternehmensseiten aus dem Bereich der kritischen Infrastrukturen sollten einem IS-Webcheck mit Testverfahren, die für Webanwendungen mit erhöhtem Schutzniveau eingesetzt werden, unterzogen werden. Bei der Bewertung der Mängel der getesteten Webanwendung muss der Prüfer die Auswirkung des jeweils gefundenen Mangels auf das Schutzniveau der kritischen Infrastruktur einbeziehen, daher sollte ein Prüfer weitreichende Kenntnisse im Bereich des jeweiligen Sektors der untersuchten kritischen Infrastruktur nachweisen, um Mängel entsprechend der Kritikalität im jeweiligen KRITIS Sektor zu bewerten.

[9] siehe auch: „BSI-Grundschutz „erweiterte Fachkenntnisse“ z. B.: „Baustein Webanwendungen 3.3 Anforderungen bei erhöhtem Schutzbedarf“ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_1_Webanwendungen.html?nn=10134826#doc10095904bodyText17

[10] siehe auch: “Das BSI Gesetz BSIG“ https://www.gesetze-im-internet.de/bsig_2009/

2.1.5 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, so 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.

2.1.6 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 qualifizierte Zertifikate für Prüfstellen oder auch über Zertifikate für das Personal wie über die Personenzertifizierung des BSI [3], Certified Ethical Hacker oder CREST [4]. Diese Verfahren enthalten praktische Prüfungen, womit die Fähigkeit zur Umsetzung eines Webapplikationstests geprüft wird. Bei dem weit verbreiteten Zertifikat des Certified Ethical Hackers [5], wird in theoretischen Prüfungen nachgewiesen, 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.

2.1.7 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. Wichtig bei der Auswahl ist, dass der Prüfer die verwendeten Tools mit allen Einsatzgebieten genau kennt und getestet hat.

2.2 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.

2.2.1 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 zusätzlichen Kosten für weiterführende Dienstleistungen 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 Beschränkung der zeitlichen, finanziellen und personellen Ressourcen nicht gewährleistet ist, dass alle vorhandenen Fehler gefunden werden.

2.2.2 NDA (Non Disclosure Agreement)

Im Vertrag sollte 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.

2.2.3 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

Dem Datenschutz wird durch das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) eine besondere Rolle in der Vorbereitung und der Durchführung, sowie der Nachbearbeitung eines IS-Webchecks zugeschrieben. Die folgenden Punkte sind bei der Beauftragung und Durchführung eines IS-Webchecks aus der Perspektive der DSGVO zu beachten.

- (1) Sofern durch einen IS-Webcheck personenbezogene Daten des Auftraggebers an den Auftragnehmer (oder Personen, deren Hilfe sich der Auftragnehmer zur Durchführung dieses Auftrages bedient) gelangen, so sind bei deren Verarbeitung die gesetzlichen Vorschriften des Datenschutzes zu beachten.
- (2) Der Auftraggeber stellt sicher, dass die in seinem Verantwortungsbereich jeweils relevanten gesetzlichen Vorschriften des Datenschutzes beachtet werden.
- (3) Der Zugriff auf erlangte personenbezogene Daten des Auftraggebers ist auf den kleinstmöglichen Kreis an Personen beim Auftragnehmer zu beschränken.
- (4) Sofern die Ergebnisse oder die Aussagekraft der Tests nicht beeinflusst werden, sind die personenbezogenen Daten zu anonymisieren.
- (5) Sofern besondere Kategorien von personenbezogenen Daten gefunden werden, verpflichtet sich der Auftragnehmer den IT-Sicherheitstest zu unterbrechen, die gefunden personenbezogenen Daten der besonderen Kategorie unverzüglich zu löschen und den

Auftraggeber über den Fund zu informieren. Der IT-Sicherheitstest wird erst fortgesetzt, wenn und soweit der Auftraggeber die personenbezogenen Daten der besonderen Kategorie aus dem IT-System entfernt oder sein IT-System so konfiguriert hat, dass ein Zugriff auf die gefunden personenbezogenen Daten der besonderen Kategorie ausgeschlossen ist.

- (6) Die personenbezogenen Daten sind – gleichgültig in welcher Form sie vorliegen (Papier, elektronischer Datenträger etc.) – nach Abschluss des Auftrages zu löschen. Dies ist dem Auftraggeber schriftlich zu bestätigen.

2.2.4 Geheimschutz

„Wenn als Verschlusssache (VS) eingestufte Informationen oder VS verarbeitende IT-Systeme durch einen IS-Webcheck betroffen sind, ist die für den Geheimschutz zuständige Stelle zu beteiligen. Sie legt die Mittel und Wege fest, wie der IS-Webcheck nach den VS-Vorschriften durchzuführen ist. Die Prüfer müssen entsprechend der VS-Einstufung sicherheitsüberprüft (siehe SÜG) sein und zum Zugang zu VS ermächtigt werden. Für die Arbeit mit Verschlusssachen in den Bundesländern existieren eigene Vorschriften."

Sicherheitsüberprüfungsgesetz (SÜG)

„Eine Person, die mit dem Umgang einer sicherheitsempfindlichen Tätigkeit betraut werden soll (Betroffener), ist vorher einer Sicherheitsüberprüfung zu unterziehen. Auf eine Sicherheitsüberprüfung nach diesem Gesetz kann verzichtet werden, wenn für den Betroffenen bereits eine gleich- oder höherwertige Sicherheitsüberprüfung durchgeführt worden ist." [11]

2.2.5 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 vermehrten Zugriffe von außen, während der Testphase auf das Netzwerk des zu testenden Ziels, kann es 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.

[11] siehe auch: „Sicherheitsüberprüfungsgesetz" https://www.gesetze-im-internet.de/s_g/index.html/

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 (neue Infrastruktur, Modernisierung der Betriebssysteme durch Patchen, Umzug der Webanwendung auf eine neue Plattform) 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 die 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, nach spätestens drei Jahren 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.

Als erste Möglichkeit wird der *nicht invasiver Schwachstellenscan* betrachtet. 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 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, welche Mängel die Webanwendung angreifbar machen. 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. Der Zugriff auf die Daten innerhalb des Fremdnetzes setzt eine entsprechende Sicherheitsüberprüfung voraus. Je nach Schutzbedarf der Informationen müssen Dienstleister und Tester ihre Vertrauenswürdigkeit nachweisen können. Die Ermächtigung zur Einsichtnahme in Verschlusssachen ist bei Bedarf durch die Vorlage einer gültigen Konferenzbescheinigung zu belegen.

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 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. Es liegt in der Verantwortung der Institution, dass die verwendeten IT-Systeme identisch aufgebaut sind. Es muss allerdings 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.
Sollten Änderungen des getesteten Ziels erfolgen, so muss im Abschlussbericht entsprechend darauf hingewiesen werden, ebenso in der fernmündlichen Information des Auftraggebers.

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 und welche Daten personenbezogen, oder ggf. nach Geheimschutz zu behandeln sind.

Die Webanwendung selbst sollte in klar abgegrenzte Funktionen unterteilt und diese beschrieben werden.

Spezielle Sicherheitsmaßnahmen bezüglich der Webanwendung selbst sollten beschrieben werden.

Liste der beteiligten IT-Systeme mit Beschreibung der Härtungsmaßnahmen

Es 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 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, die den IS-Webcheck durchführen, auch über die im Angebot beschriebenen Qualifikationen verfügen. Es sollten nur Personen als Vertreter akzeptiert werden, die vergleichbare Qualifikationen nachweisen.

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 weiterführende Literatur verwiesen, 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 3.2. „Festlegung des Prüfumfangs“) 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.

4.2.1 Anfangsgespräch

Am Tag vor Beginn der Tests, oder bereits einige Tage vorher, sollte ein kurzes Gespräch mit dem Auftraggeber/Hoster und dem beteiligten technischen Personal stattfinden. Da der IS-Webcheck nicht 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.

4.2.2 Prüfbedingungen

Danach werden die Prüfbedingungen für den Test in Augenschein genommen. Die Prüfer stellen fest, 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 für die Dauer des Tests zu Verfügung stehen.

4.2.3 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 getesteten Aspekte zu vermitteln. Die Reihenfolge der Module kann individuell festgelegt werden, auch können einzelne Module mehrfach durchgeführt oder gleichzeitig abgearbeitet werden. Dies geschieht, sobald 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 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.

Anhand der Dokumentation des Auftraggebers über die Funktionalität der Webanwendung wird auch der Sicherheitsbedarf der ein- und ausgegebenen Daten einer Webanwendung dem Prüfer übermittelt. Anhand des Sicherheitsbedarfs der verarbeiteten Daten wird die Webanwendung auf die mögliche Verschlüsselung geprüft.[12] 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 eine Übertragung der verarbeiten Daten über ‚HTTPS' nicht grundsätzlich sinnvoll sei. Wenn eine HTTPS-Verbindung angeboten wird, sollten alle Inhalte ausschließlich über HTTPS verfügbar sein. Sogenannter Mixed Content sollte nicht verwendet werden.

Viele Webanwendungen liefern zunächst ein großes Informationsangebot, aber auch viele Interaktionsmöglichkeiten mit der Anwendung, Jede Interaktion des Anwenders beinhaltet die Möglichkeit zur Manipulation der übertragenen Informationen. Ist eine gute Absicherung des Webangebotes implementiert, dann ist höchstwahrscheinlich nur erwünschtes Verhalten zugelassen, bei schlechterer Absicherung sind hier die möglichen Angriffspunkte zu finden. Diese Möglichkeiten

[12] siehe auch: "Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile&v=4

sollen an dieser Stelle identifiziert und in den folgenden Modulen genauer untersucht werden. 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 anhand der Antwort der Webanwendung, ob eine Schwachstelle vorliegen kann. 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. So wird Dritten eine Möglichkeit gegeben die Ergebnisse der gefundenen Schwachstellen nachzuvollziehen.

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
- Ausgabekodierung
- Session Handling
- Zugriffskontrolle
- Verschlüsselung
- Fehlerhandling
- Absicherung der beteiligten Datenbanken und Anwendungen
- Absicherung von Dateiuploadmöglichkeiten und weiteren Interaktionsmöglichkeiten
- versteckte Parameter/Verzeichnisse
- Weitereichende Absicherung einer Webanwendung mit erhöhtem Schutzniveau

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 verdeutlicht 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 [10] und werden an dieser Stelle nicht ausführlich beschrieben.

Eingabevalidierung und Ausgabekodierung

Jedes Eingabefeld, in das der Anwender Eingaben tätigen kann, wurde dafür konzipiert, Daten an eine Anwendung und die ggf. dahinter liegenden Datenbanken weiterzugeben. Ist die Eingabe unzureichend abgesichert, können hierüber Angriffe getätigt werden. Webanwendungen werden von Web-Browsern verwendet, sodass Benutzer beliebige Eingabedaten an den Server übermitteln können. Werden schadhafte Eingaben eines Angreifers von der Webanwendung verarbeitet, können möglicherweise Schutzmechanismen umgangen werden.

Unzureichende Validierung der Eingabedaten können zu Angriffen führen, die Unbefugten Zugriff auf das Betriebssystem oder auf Hintergrundsysteme ermöglichen. Bei einem erfolgreichen Angriff können schützenswerte Daten unautorisiert ausgelesen oder manipuliert werden.

Nachdem die Webanwendung die Eingabedaten erfolgreich verarbeitet hat, werden üblicherweise wieder Daten ausgegeben. Die Ausgabedaten werden an den Browser des Benutzers oder an nachgelagerte Systeme weitergereicht. Werden die Daten vor der Ausgabe nicht ausreichend kodiert, könnten die Ausgaben Schadcode enthalten, der auf den Zielsystemen interpretiert oder ausgeführt wird.[13]

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 und Web-Services sind im Regelfall so konzipiert, dass mehrere Anwender gleichzeitig mit ihr interagieren können.

Webanwendungen und Web-Services verwenden in der Regel das zustandslose Protokoll zur Übertragung der Daten. Es unterstützt keine Zuordnung zusammengehörender Anfragen zu einem Benutzer. Das Session-Management einer Webanwendung oder eines Web-Service hat zur Aufgabe, die Sitzungen zu verwalten und neue Session-IDs zu vergeben.

Wenn sich der Benutzer bei der Webanwendung oder dem Web-Service angemeldet hat, ist die vergleichbar mit seinen Zugangsdaten. Die Webanwendung identifiziert mit ihr bei jedem Seiten- oder Dienstaufruf den Benutzer und ordnet ihn einer (gegebenenfalls privilegierten) Sitzung zu.

Nutzen Unbefugte die Session-ID, werden sie als legitime Benutzer identifiziert und können die Anwendung oder den Dienst im Namen des Opfers verwenden.[14]

Authentisierung und Autorisierung
Wenn eine Webanwendung sensible Daten verarbeitet, so wird der Zugriff auf diese Daten 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 benötigten Daten oder Bereiche der Webanwendung sichten oder bearbeiten kann. Angreifer versuchen häufig, auf Funktionen oder Daten von Webanwendungen zuzugreifen, die nur für eine eingeschränkte Benutzergruppe verfügbar sind. Ist die Autorisierung fehlerhaft umgesetzt, kann ein Angreifer die Berechtigungen eines anderen Benutzers mit umfangreicheren Rechten erlangen und auf geschützte Bereiche und Daten zugreifen. Das geschieht üblicherweise, indem ein Angreifer seine Eingaben gezielt manipuliert, indem er (nicht vorgesehene) Befehle oder Anweisungen in die Textfelder eingibt.[15]

---

[13] siehe auch: „Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Webanwendungen/Baustein_Webanwendungen-B5_21.pdf?__blob=publicationFile&v=1

[14] siehe auch: „Unzureichendes Session-Management bei Webanwendungen“[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Webanwendungen/Baustein_Webanwendungen-B5_21.pdf?__blob=publicationFile&v=1

[15] siehe auch: „Authentisierung bei Webanwendungen“[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Webanwendungen/Baustein_Webanwendungen-B5_21.pdf?__blob=publicationFile&v=1

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 können. Daher sollte alles nur verschlüsselt übertragen werden.[16] Der Einsatz von Geschäftsprozessen mit erhöhtem Schutzbedarf benötigen verstärkte Sicherheitsmaßnahmen im Bereich der Verschlüsselung. Diese werden im Kryptokonzept dargestellt. [17]

Fehlerhandling

Entwickler möchten bei Eintritt eines Fehlers so viele Informationen über das Event wie möglich erhalten, um den Fehler schnell beseitigen zu können. Erhalten Angreifer Zugang zu diesen umfangreichen Informationen können daraus Angriffsszenarien erstellt werden.[18] „Webseiten und Daten, die von einer Webanwendung generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu Datenbanken oder Versionsständen von Frameworks. Diese Informationen können es einem Angreifer erleichtern, gezielte Angriffe auf die Webanwendung durchzuführen.“[19]

Absicherung der beteiligten Datenbanken und Anwendungen

Wenn ein Angreifer Funktionen einer Webanwendung automatisiert nutzt, kann er zahlreiche Vorgänge in kurzer Zeit ausführen und so auf Wiederholung basierende Angriffe gegen die Webanwendung effizient durchführen. Mithilfe eines wiederholt durchgeführten Login-Prozesses können z. B. gültige Kombinationen aus Benutzernamen und Passwort systematisch ermittelt (Brute-Force) oder Listen mit gültigen Benutzernamen erzeugt werden (Enumeration). Darüber hinaus kann das wiederholte Aufrufen von ressourcenintensiven Funktionen (z. B. komplexe Datenbankabfragen) für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden.[20]

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

---

[16] siehe auch: „ Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile&v=4

[17] siehe auch : „Kryptokonzept“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5

[18] siehe auch: „Offenlegung sicherheitsrelevanter Informationen bei Webanwendungen“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Webanwendungen.pdf?__blob=publicationFile&v=11

[19] siehe auch: „Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen“ [2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5

[20] siehe auch: „Missbrauch einer Webanwendung durch automatisierte Nutzung“ [2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5

Webanwendungen umgesetzt und damit ausgenutzt werden können. Es könnte der Mail-Versand von einer Funktion als SPAM-Relais genutzt werden.[21]

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.

Funktionen des Browsers zur Steigerung der Absicherung gegen mögliche Angriffe

Der Mindeststandard des BSI für den Einsatz sicherer Web-Browser gibt vor, welche Browser für den sicheren Datenaustausch im Bereich der Bundesbehörden zu nutzen sind. Die Anwendung des Web-Browsers enthält Funktionen die den Datenaustausch schützen und weniger angreifbar machen. Die Funktionalität des Browsers wird durch entsprechende Response-Header Einträge aktiviert. Im Rahmen des IS-Webchecks wird die Kommunikation zwischen Client und Server auf entsprechende Header-Einträge geprüft.[22] Die Mitigation durch Konfiguration des Webservers bietet zahlreiche Einstellungen, um Angriffe zu vermeiden. Das zustandslose HTTP-Protokoll bietet eine große Zahl von Einstellmöglichkeiten, die Angriffe erschweren. Der Client wertet diese Informationen aus und nutzt die implementierten Sicherheitsmechanismen.[23]

Weiterreichende Absicherung einer Webanwendung mit erhöhtem Schutzniveau

Im Rahmen des BSI Grundschutz werden exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Durch den IS-Webcheck wird der sachgemäße Einsatz der Techniken und die Konfiguration der Schutzmechanismen bei Webanwendungen mit erhöhtem Schutzbedarf überprüft.[24] Über die Standardmaßnahmen zur Absicherung einer Webanwendung hinaus, die sich besonders an Absicherung von Webanwendungen mit erhöhtem

[21] siehe auch: „Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=9

[22] siehe auch: „Mindeststandard des BSI für sichere Web-Browser nach §8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 20.03.2017" https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/Sichere_Web-Browser/Sichere_Web-Browser_node.html

[23] siehe auch: „Sichere Konfiguration eines Webservers" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Webserver.pdf?__blob=publicationFile&v=9

[24] siehe auch: „IT Grundschutz Webanwendungen - Anforderungen bei erhöhtem Schutzbedarf"[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_1_Webanwendungen.html?nn=10134826#doc100959

Schutzbedarf richten. Diese exemplarischen Vorschläge gemäß dem BSI Grundschutz werden auch als Teil der Prüfung einer Webanwendung mit normalem Schutzbedarf angewandt.[25]

Einsatz von Web Application Firewalls

Zur Filterung von Daten auf höheren Protokollebenen, können Institutionen auf Web Application Firewalls (WAF) zurückgreifen. Wird eine WAF eingesetzt, sollte die Konfiguration auf die zu schützende Webanwendung angepasst werden. Es wird empfohlen, die Konfiguration der WAF nach jedem Update der Webanwendung zu prüfen. Das Regelwerk der Konfiguration einer eingesetzten WAF wird im Rahmen eines IS-Penetrationstests auf mögliche Fehler untersucht.

Verhinderung der Blockade von Ressourcen

Zum Schutz vor Denial-of-Service-(DoS)-Angriffen sollten ressourcenintensive Operationen vermieden und besonders abgesichert werden. Ebenso sollte ein möglicher Überlauf von Protokolldaten bei Webanwendungen überwacht und verhindert werden. SOAP-Nachrichten sollten anhand eines entsprechenden XML-Schemas validiert werden. Bei kritischen Diensten und Anwendungen sollte geprüft werden, mit Anti-DoS-Dienstleistern zusammenzuarbeiten.

Modul 3 – Logische Fehler/Konfigurationsfehler

Geschultes Personal in der Softwarentwicklung

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 und Entwickler, 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 für die Erweiterung einer Webanwendung eingeplant, ist die dafür vorgesehene Technik veraltet, oder die geplante Erweiterung nicht mehr gefragt. Ausreichend Zeit wäre allerdings notwendig, um das komplexe Gebilde eines Webauftritts fehlerfrei 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. Die Webanwendung sollte im Rahmen eines IS-Webchecks auf den Einsatz nicht benötigter Dienste, fehlerhafter, oder veralteter Software überprüft werden.[26]

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

[25] siehe auch: „3.3 Anforderungen bei erhöhtem Schutzbedarf“ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_3_1_Webanwendungen.html;jsessionid=3C759ECA61C8D79AF3E2354D3A6F528F.2_cid369?nn=10134826#doc10095904bodyText17

[26] siehe auch: „Software Entwicklung“ [2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Softwareentwicklung.pdf?__blob=publicationFile&v=16

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, um unerwünschte Nebeneffekte zu vermeiden.

4.2.4 Abschlussgespräch

Nach Abschluss der Tests sollte ein Gespräch zwischen den Prüfern und den Ansprechpartnern seitens der Auftraggeber stattfinden. Ziel ist es, 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. Das Abschlussgespräch eines IS-Webchecks gibt die Möglichkeit auf eklatante Mängel hinzuweisen, damit die Anwendung unmittelbar nachgebessert, oder vom Netz genommen werden kann.

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.

Das BSI empfiehlt, die Vorstellung der Schwachstellen im Abschlussgespräch nur unter Vorbehalt stattfinden zu lassen. 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 muss eine Vertraulichkeitskennzeichnung 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 der Prüfmodule 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 CVSSv3 [11] oder DREAD [12] von Microsoft herangezogen werden.
Die Einstufung der gefundenen Schwachstellen bzgl. der Kritikalität erleichtert es den Administratoren, eine Reihenfolge bei der Behebung der Schwachstellen einzuplanen.

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.

Sollte bei einem erneuten IS-Webcheck einer Webanwendung, welche im Regelfall nach spätestens drei Jahren erfolgt, Mängel festgestellt werden, die auch im vorhergehenden Bericht aufgelistet wurden, so werden diese Mängel um eine Stufe in der Kritikalität erhöht. Ein Mangel der eine sofortige Reaktion erfordert hätte und erneut nachgewiesen wird, führt zum Abbruch des IS-Webchecks.

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

Kritischer Mangel

Eine Schwachstelle wird mit der Kategorie „kritischer Mangel“ bewertet, wenn eine direkte Bedrohung für die Sicherheit der Webapplikation vorliegt. Weiter kann ein Verstoß gegen die Mindeststandards des BSI als kritischer Mangel bewertet werden. Die Reaktion auf eine solche Bedrohung sollte **sofort** erfolgen

Schwerwiegender Mangel

Eine Schwachstelle wird mit der Kategorie „schwerwiegender Mangel“ bewertet, wenn eine schwerwiegende Gefährdung für die Sicherheit der Webapplikation erkannt wird. Die Reaktion auf eine solche Bedrohung sollte **kurzfristig** erfolgen

Mangel

Eine Schwachstelle wird mit der Kategorie „Mangel“ bewertet, wenn eine unbestimmte Gefährdung für die Sicherheit der Webapplikation erkannt wird. Die Reaktion auf eine solche Bedrohung sollte **mittelfristig** erfolgen.

Zur Information

Eine Schwachstelle wird mit der Kategorie „Zur Information“ bewertet, wenn ein Verbesserungspotenzial für die Sicherheit der Webapplikation erkannt wird. Die Reaktion sollte **langfristig** erfolgen.

Das BSI empfiehlt, die ausführliche Beschreibung eines Mangels 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

Im Folgenden werden dem Auftraggeber und dem Auftragnehmer zwei Listen in tabellarischer Form zur Verfügung gestellt, anhand derer die Beauftragung und die Durchführung eines IS-Webchecks unterstützt wird.

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	
	Einarbeitungsphase	

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

5.1.2 Hilfestellung zur Durchführung eines IS-Webchecks

Diese Checkliste soll Prüfern helfen die organisatorischen und fachlichen Rahmenbedingungen, die bei einem IS-Webcheck erfüllt werden müssen, strukturiert durchzuführen.

Sollten einzelne Pakete nicht bearbeitet werden, so sollte der Grund dafür mit dem Auftraggeber abgesprochen und dokumentiert werden.

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/Geheimschutzbeauftragten 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-	

Arbeitspaket	**Unterpaket 1**	**Unterpaket 2**	**Unterpaket 3**	**Erforderliche Personen**	**Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)**
				Sicherheitsverant-wortlicher oder Fachverantwortliche)	
	Prüfumgebung			Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverantwortlicher 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-Sicherheitsverantwortlicher oder Fachverantwortliche)	
			Verschlüsselung	Prüfer, Ansprechpartner Institution/Hoster (IT-Sicherheitsverant-wortlicher oder Fachverantwortliche)	
			Fehlerhandling	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)	
			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			

Arbeitspaket	**Unterpaket 1**	**Unterpaket 2**	**Unterpaket 3**	**Erforderliche Personen**	**Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)**
		Technische Beschreibung der Schwachstellen mit Empfehlungen und Einstufung der Kritikalität			

5.2 Ablaufplan

Dieser Ablaufplan soll helfen, die organisatorischen und fachlichen Rahmenbedingungen, die ein IS-Webcheck erfüllen muss, 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 Beeinträchtigungen zu erwarten sind.

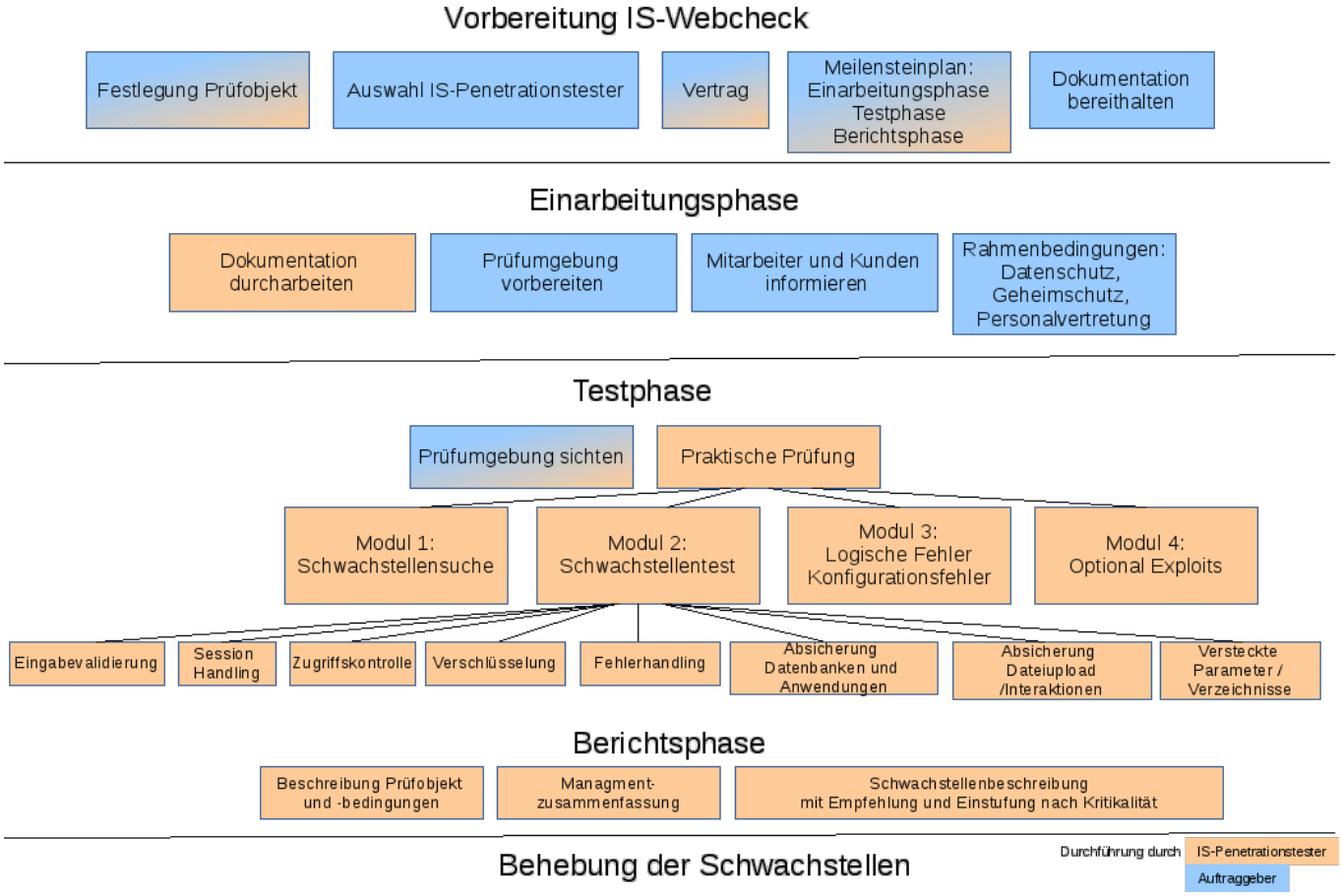

Abbildung 3 Ablauf eines IS-Webcheck

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.[27]

Angriff/Angreifer

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

APT

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Buffer Overflow

Werden einem Modul über eine Schnittstelle mehr Daten als erwartet übergeben, so kann es zu einem sogenannten „Buffer Overflow“ kommen. Wenn das Modul nicht die Länge der übermittelten Daten prüft, werden die Daten über den vorgesehenen Bereich hinaus geschrieben und somit die Speicherstruktur (Heap oder Stack) zerstört. Durch geeignete Codierung der Daten kann zudem der Stack gezielt manipuliert werden, sodass die Ausführung schadhaften Codes möglich ist.

Cross-Site Scripting Angriff (XSS)

Cross-Site-Scripting-Schwachstellen entstehen, wenn Benutzereingaben in einer Webanwendung ungefiltert durch den Server verarbeitet und an andere Clients zurückgegeben werden. Ein Angreifer hat damit unter Umständen die Möglichkeit, Programmcode wie JavaScript im Kontext des Benutzers einer Webseite auszuführen. Dies lässt sich unter anderem ausnutzen, um den Inhalt von Webseiten für einen Benutzer zu ändern oder auf Inhalte wie Cookies zugreifen zu können, um an Session-Informationen zu gelangen

Es gibt drei Arten von XSS-Angriffen Attacken: non-persistent, persistent und DOM-based.

[27] siehe auch: „IT Grundschutz - Glossar und Begriffsdefinitionen“ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

DoS

Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

Exploit

Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

IS-Penetrationstest

Penetration Testing bezeichnet den Sicherheitstest eines Computersystems oder Netzwerks durch eine damit vom Inhaber beauftragten und hierzu berechtigten Person oder Organisation mittels eines Audits oder Techniken (Hacking), die ein unautorisierter Angreifer verwenden würde, um in ein System einzudringen.

IS-Revision

Die IS-Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-)Richtlinien. Die Revision sollte unabhängig und neutral sein.

IS-Webcheck

Ein WebCheck stellt einen Teilbereich von Penetrationstests dar. Dabei werden Webauftritte oder deren Teilbereiche mit automatisierten Verfahren auf Schwachstellen getestet. Hierbei wird – wenn möglich – über das Internet auf die Angebote zugegriffen, um vergleichbare Voraussetzungen wie bei einem Angriff zu nutzen.

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, 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 Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Spoofing

Spoofing (von to spoof, zu deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

SQL-Injection

SQL-Injection ist eine Cyber-Angriffstechnik, welche eine Sicherheitslücke im Zusammenhang mit SQL-Datenbanken ausnutzt um Zugriff auf die Datenbank selbst oder den die Datenbank bereitstellenden Server zu erlangen.

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

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

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

[6] Leitfaden IS-Penetrationstest

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

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

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

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

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

[11] NVD Common Vulnerability Scoring System Support v3 (CVSSv3)
https://www.first.org/cvss/specification-document

[12] Microsoft Thread Modeling (Einstufung mit DREAD)

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

[13] BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=6/