
# Best Practice: Projektierung der Sicherheitsprüfung von Webanwendungen

Version 1.01, 08. Oktober 2009

Autor: *OWASP German Chapter* unter Mitwirkung von (alphabetische Reihenfolge):
Marco Di Filippo
Tobias Glemser
Achim Hoffmann
Barbara Schachner
Dennis Schröder
Feiliang Wu

## Über ...

Dieses Dokument wurde vom *OWASP German Chapter* erarbeitet. Die Autoren sind Mitarbeiter von Unternehmen, die Penetrationstests von Webanwendungen durchführen, bzw. auf Kundenseite tätig sind und die Projektierung übernehmen.

## Autoren (alphabetische Reihenfolge)


| | | |
|---|---|---|
| Marco Di Filippo | marco.difilippo@csnc.ch | Compass Security AG |
| Tobias Glemser | tglemser@tele-consulting.com | Tele Consulting security \| networking \| training GmbH |
| Achim Hoffmann | ah@securenet.de | SecureNet GmbH |
| Barbara Schachner | barbara.schachner@siemens.com | Siemens AG - Corporate Technology |
| Dennis Schröder | d.schroeder@tuvit.de | TÜV Informationstechnik GmbH |
| Feilang Wu | feiliang.wu@siemens.com | Siemens AG - Corporate Technology |


## Terminologie

Die in diesem Dokument verwendeten Fachbegriffe sind nicht weiter erklärt, sondern werden als bekannt vorausgesetzt. Auf ein Glossar wurde bewusst verzichtet damit der Umfang überschaubar bleibt und sich der Inhalt auf das eigentliche Thema – die Beschreibung der Anforderungen – konzentriert.

Ausführliche Begriffserklärungen und weiterführende Beschreibungen im Zusammenhang mit WAS – Web Application Security – finden sich in:

- http://www.owasp.org/index.php/Category:Attack OWASP Category:Attack
- http://www.owasp.org/index.php/Category:Threat OWASP Category:Threat
- http://www.owasp.org/index.php/Category:Vulnerability OWASP Category:Vulnerability
- http://projects.webappsec.org/Threat-Classification-Reference-Grid
  WASC Web Application Security Consortium: WASC Threat Classification
- http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.de.pdf
  WASC Web Application Security Consortium: Web Security Threat Classification

## Lizenz



# Inhaltsverzeichnis

# 1 Einführung und Zielsetzung dieses Dokuments

## 1.1 Einführung

Die Prüfung der Sicherheit von Webanwendungen wird mittlerweile von vielen Unternehmen als erforderlicher Schritt anerkannt. Insbesondere für die erstmalige Prüfung ist es für den Betreiber von Webanwendungen schwierig, ein entsprechendes Projekt aufzusetzen. Es gilt, zum einen den Projektfokus klar zu definieren, um eine Vergleichbarkeit von Angeboten zu erzielen und zum anderen die Expertise der Dienstleister möglichst transparent bewerten zu können.

## 1.2 Begriffsdefinitionen

Kunde: Kunde im Sinne dieses Dokuments ist ein Betreiber von Webanwendungen, der auf der Suche nach einem Dienstleister (intern oder extern) für die Sicherheitsprüfung der Webanwendungen ist.

Interner oder externer Dienstleister: Abteilung oder Unternehmen mit Expertise bei der Durchführung von Sicherheitsprüfungen von Webanwendungen.

Webanwendung: Auf Webtechnologien aufsetzende Anwendung (z. B. klassische Internetpräsenz, Web-API, Web-Frontend von Anwendungsservern). Dies können einfache Anwendungen (meist statische Inhalte auf einem Server lagernd), aber auch komplexe dynamische Anwendungen (mehrere Server, Loadbalancer, 3-Tier-Aufbau, usw.) sein.

## 1.3 Zielgruppe und Zielsetzung

Zielgruppe sind vor allem Betreiber von Webanwendungen, die eine Sicherheitsüberprüfung der Webanwendung projektieren möchten. Diesen wird mit Hilfe dieses Dokuments ein Leitfaden für den gesamten Prozess an die Hand gegeben. Dieser Leitfaden beginnt bei der Definition der Projektziele, über die Projektplanung bis hin zur Ausschreibung. Die richtige Dienstleisterauswahl hängt von vielen Faktoren ab und ist für jeden Kunden und jedes Projekt unterschiedlich sowie auf den ersten Blick für die Kundenseite selten transparent. Daher wird im Rahmen dieses Dokuments versucht eine generische Hilfestellung zu geben, um mit transparenten Methoden den geeignetsten Dienstleister zu identifizieren.

## 1.4 Abgrenzung

Es wurde versucht, das Dokument so „untechnisch“ wie möglich zu formulieren und nicht den technischen Inhalt anderer Veröffentlichungen zu wiederholen. Sofern es dem Gesamtverständnis dient, wurden einige technische Erläuterungen aufgenommen, insbesondere bei der Beschreibung der Prüfarten. Diese sollen jedoch nur ein rasches Verständnis für Begrifflichkeiten und Abgrenzungen wecken und nicht in Gänze erörtert werden. Daher sind Verweise auf weitere Dokumente angegebenen, die einen hohen, technischen Detaillierungsgrad haben.

## 1.5 Aktualisierungen

Das Projektteam freut sich jederzeit über konstruktives Feedback und ist bemüht, dies für künftige Versionen aufzunehmen. Die aktuelle Version des Dokuments findet sich auf der Projektwebseite. Feedback kann an einen der an der Erstellung des Dokuments beteiligten Autoren gesendet werden.

# 2 Anforderungen

Wenn die Entscheidung zur Sicherheitsüberprüfung einer Webanwendung getroffen wurde, sind aus Sicht des Kunden bereits Anforderungen bekannt, auch wenn diese ggf. noch nicht vollständig definiert sind. Ebenso bestehen meist gewisse Vorstellungen, was die Ansprüche an den Dienstleister anbelangt.

Die Folgekapitel sind entsprechend aufgeteilt. Kapitel 2.1 beschäftigt sich mit den Fragestellungen, die ein Kunde in sein Lastenheft aufnehmen kann. Kapitel 2.2 stellt dar, welche Mindestanforderungen an Dienstleister gestellt werden und mit welchen Methoden das Anforderungsprofil geprüft werden kann.

## 2.1 Kundenseite

Möchte man die Prüfung einer Webanwendung durchführen lassen – durch interne oder externe Kräfte – ist die Projektierungsphase für den Erfolg des Projekts entscheidend. Hier muss der Kunde verbindliche Vorgaben für den Umfang, die Art der Prüfung und die anzuwendende Methodik festlegen. Grobe Fehler in dieser Phase sind während der Projektdurchführung nur schwer auszugleichen. Darüber hinaus ist eine Festlegung auf Randbedingungen für die Vergleichbarkeit von Angeboten wichtig. Wer Wasser wünscht und nachher Wein bekommt (und bezahlen soll) ist ebenso wenig zufrieden gestellt wie im umgekehrten Fall.

Die folgenden Kapitel geben daher entsprechende Hinweise auf häufige auftretende Schwierigkeiten und Empfehlungen zur Vermeidung eventueller Missverständnisse.

Da auch in der Projektierungsphase bereits grundlegende Kenntnisse notwendig sind, kann es insbesondere bei der ersten derartigen Untersuchung sinnvoll sein, im Rahmen eines Workshops gemeinsam mit internen oder externen Experten eine Vorgehensweise zu entwickeln. Hinweise zur Dienstleisterauswahl finden sich in Kapitel 2.2. Sofern ein externer Dienstleister an der Entwicklung des Pflichtenhefts beteiligt ist, darf dieser zur Wahrung der Neutralität und aufgrund evtl. gesetzlicher Vorschriften nicht an der resultierenden Ausschreibung teilnehmen.

### 2.1.1 Art der Prüfung

Für die Projektierung und vor Allem für die Ausschreibungsphase ist es entscheidend festzulegen, welche Art der Prüfung gewünscht wird. Es gibt sehr unterschiedliche Prüfansätze, die jeweils einer unterschiedlichen Motivationslage entspringen und sich in Methodik, Umfang, Zeitaufwand, Ergebnistiefe und Aussagekraft unterscheiden.

Es wird empfohlen, dass sich die Ausschreibung an anerkannten Prüfstandards oder zumindest an deren Methodik orientiert. Somit werden Vorgaben formuliert und eine grundlegende Vergleichbarkeit der Durchführung geschaffen.

Ziel einer Untersuchung ist neben der Transparenz der Methoden die Wiederholbarkeit der Prüfungen. Diese Forderung sollte in den Ausschreibungsunterlagen beinhaltet sein. IT-Sicherheit wird durch Transparenz erst belastbar, ansonsten lässt sich das Ergebnis von niemand außer dem Prüfer selbst in Umfang und Aussagekraft bewerten.

#### 2.1.1.1 Vulnerability-Assessment (VA) / Penetrationstest der Webanwendung

Um einen Angreifer auf eine Webanwendung zu simulieren, kann man auf die Methodik eines Vulnerability-Assessment (VA) oder Penetrationstests zurückgreifen. Ein Vulnerability Assessment wird in diesem Dokument als Untersuchung verstanden, die ausschließlich bekannte Schwachstellen identifiziert (vorwiegend toolgestützt). Wird diese Vorgehensweise durch manuelle Methoden sowie Erfahrung und Kreativität des Prüfers ergänzt, so wird dies als Penetrationstest bezeichnet.

Es gibt unterschiedliche Ansätze zur Durchführung von Penetrationstests. Einige sind sehr allgemein formuliert, um auf möglichst jede IT-Umgebung anwendbar zu sein. Eine anerkannter Ansatz ist das *Durchführungskozept für Penetrationstests* des Bundesamts für Sicherheit in der Informationstechnik (BSI: www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf). Einen weiteren Standard bietet das *Open Source Security Testing Methodology Manual* der ISECOM (http://www.osstmm.org/), welches international häufig referenziert wird. Viele Beratungsunternehmen haben entsprechend ihrer eigenen Schwerpunkte teilweise eigene Methoden entwickelt, die jedoch häufig auf Standards aufbauen und zu diesen kompatibel sind.

Spezifischere Beschreibungen für die Durchführung von Penetrationstests auf Webanwendungen finden sich z. B. im *OWASP Testing Guide* (http://www.owasp.org/index.php/Category:OWASP_Testing_Project). Ein allgemeinerer, dennoch webanwendungsspezifischer Ansatz, der mehrere Methoden vereint, ist der *OWASP Application Security Verification Standard* (http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project).

Eine generelle Unterscheidung wird zwischen Black- und Whitebox-Prüfungen gemacht. Dies eint die Standards und ist für die Projektierung ein entscheidender Faktor. Mit der Definition eines Kenntnis-Standes wird ein Angriffstyp simuliert.

In Blackbox-Prüfungen gibt der Kunde dem Dienstleister meist keine oder nur sehr leicht zu recherchierende Informationen zur Zielanwendung. Das reine Bereitstellen von Anmeldedaten wird in diesem Dokument weiterhin als Blackbox-Test betrachtet. Blackbox-Untersuchungen sind grundsätzlich dynamische Untersuchungen, da die Tests gegen das laufende System gefahren werden. Der Quellcode steht in diesen Untersuchungen nicht zur Verfügung. Daher schlüpfen die Dienstleister hier in die Rolle des Angreifers ohne nähere Kenntnisse der IT-Infrastruktur und versuchen die Anwendung zu kompromittieren. Der Vorteil ist, dass der Kunde ein Bild darüber bekommt, wie leicht die Anwendung für Externe angreifbar ist. Der Nachteil ist, dass der Dienstleister nur mit diesem Kenntnisstand ausnutzbare Schwachstellen finden kann. Schwachstellen, die erst mit einem besseren Kenntnis-Stand (z. B. Architektur) ausgenutzt werden können, werden normalerweise nicht identifiziert. Der Kunde muss davon ausgehen, dass ein Angreifer einen frei definierten Zeitrahmen hat, nach Schwachstellen zu suchen und daher gegenüber den Dienstleistern im Vorteil ist.

Weiterhin muss sich der Kunde gründlich überlegen, ob er Blackbox-Untersuchungen von Produktivsystemen in Auftrag gibt, anstatt ein Testsystem mit entsprechenden Testdaten bereitzustellen. Bestimmte Tests können das Produktivsystem selbst in einen funktional instabilen Zustand bringen oder sogar Produktivdaten löschen, ändern und für Dritte einsehbar machen. Allerdings lässt sich diese Gefahr bei der Durchführung durch die Methodik einschränken.

Bei Whitebox-Untersuchungen bekommt der Dienstleister vom Kunden umfassende Informationen über die Anwendung. So lässt sich beispielsweise der Angriff aus Sicht eines externern Vertragspartners oder eines Mitarbeiters simulieren. Der Vorgehensweise sind jedoch Grenzen gesetzt, da sich z. B. der Angriffstyp Administrator aufgrund der Vielzahl der Kenntnisse eines Administrators oder gar eines Administratoren-Teams kaum real anwenden lässt.

Es gilt also, für die jeweilige Bedürfnislage des Kunden eine optimale Wissenslage und einen guten Wissenstransfer der Informationen an den Dienstleister zu gewährleisten.

Wichtig ist bei allen Prüfungen, dass ohne spezielle Prüfprogramme keine ernsthafte Prüfung erfolgen kann. Der Umfang von Webanwendungen übersteigt heute im Regelfall deutlich den Umfang und die Komplexität, die eine manuelle Prüfung erlauben würden. Dennoch ist die manuelle Prüfung der Webanwendung, ebenso wie die zusätzliche manuelle Verifikation aller Ergebnisse, notwendig.

Der Prüfumfang kann über die reine Prüfung der Webanwendung hinaus definiert werden. So können z. B. zusätzlich netzbasierte Penetrationstests zum Einsatz kommen, die den Webserver-Dienst, Datenbankserver, Firewalls usw. mit einbeziehen.

Ob eine Aufteilung, also Modularisierung der Prüfungen, sinnvoll ist, hängt vom jeweiligen Szenario ab. Insbesondere, wenn viele Dienste betrieben werden, kann die Modularisierung einen Effizienzgewinn bedeuten.

Ebenfalls zu klären ist die Frage, ob Denial-of-Service-Angriffe (DoS) erfolgen sollen. Diese zielen darauf ab, durch Ausnutzung von Schwachstellen oder Flutung von Systemen bzw. Diensten mit Anfragen eine Nichterreichbarkeit herbeizuführen. Dies ist allerdings in den wenigsten Fällen wirklich sinnvoll. Besser ist es, Spezifikationen zur Nutzlast zu erstellen und die maximale Nutzlast prüfen zu lassen. Dies sollte bei richtiger Umsetzung der Spezifikationen nicht zum Ausfall führen.

**SaaS - Software as a Service**

Neben der üblichen Form, dass der Dienstleister die Sicherheitsüberprüfung explizit auf Nachfrage anbietet und erbringt, gibt es noch die Möglichkeit, dass die Sicherheitsüberprüfungen durch – mehr oder weniger – vollständig automatisierte Dienste erfolgen. Das Stichwort hierzu ist SaaS und soll im Folgenden kurz beschrieben werden.

SaaS (Software as a Service) ist ein Software-Distributionsmodell, welches Software als Dienstleistung, basierend auf Internettechniken, bereitstellt (auch bekannt als ASP - Application Services Provider). D. h. die Software wird von einem Dienstleister über das Internet betrieben, womit eine Installation beim Kunden (Konsument) entfällt.

Werden Sicherheitsprüfungen von Webanwendungen als automatische, regelmäßige Dienstleistung angeboten, dann handelt dabei es sich im Wesentlichen um einen genau definierten Scan der Website nach Schwachstellen.

Dieses Geschäftsmodell bietet eine Alternative sowohl zum Kauf eines Scan-Tools als auch eines einmaligen Penetrationstests als Dienstleistung.

Die Vorteile auf Kundenseite gegenüber der Dienstleistung per Einzelauftrag sind:

- einmaliger Aufwand für die Projektierung, und dadurch kostengünstiger,
- einfache Wiederholung von Sicherheitsüberprüfungen,
- regelmäßige Tests, und dadurch fortlaufende Kenntnis über den Sicherheitsstand.

Die oftmals versprochene enorme Kostenreduzierung gegenüber den Alternativen hat aber auch einige Nachteile in Bezug auf die Sicherheitsprüfung selbst und das damit verbundene Umfeld. Besonders beachten sollte man:

- Die Einführung von SaaS kann beeinträchtigt werden, weil innerhalb des Unternehmens (Kunde) Bedenken bzgl. der Vertrauenswürdigkeit und der Kontrolle des Anbieters bestehen, da dieser automatisiert in den Besitz sensitiver Daten und Schwachstellen kommt. Hier muss also ein erhöhtes Maß an Schutzvorkehrungen gegen Missbrauch getroffen werden.
- Was passiert mit den Daten des/der Tests, wenn der Dienstleister z. B. insolvent oder veräußert wird.
- Die zu testenden Anwendungen müssen i. d. R. über das öffentliche Internet zugänglich sein.
- Aufbau von z. B. Firewallregeln, VPN-Tunneln oder Einrichtung von speziellen Aplication-Proxies für die Scans ist ein zusätzlicher Aufwand auf Seiten des Kunden.

Weiter muss sich der Kunde überlegen, ob bei regulären, sich wiederholenden Scans vorhandene IDS/IPS und insbesondere WAFs deaktiviert werden müssen oder als Teil des Gesamtsystems mitgetestet werden sollen.

Eine regelmäßige, wiederholte Sicherheitsprüfung in Form von SaaS wird man wohl für die produktiven Webanwendungen einrichten. Im Gegensatz zu den üblichen Penetrationstests, die auf einer Labor- oder Referenzplattform stattfinden, ist zu beachten, dass der normale Betrieb durch den erhöhten Durchsatz gestört wird.

Entscheidet man sich für SaaS, dann gelten dieselben Regeln und Empfehlungen zur Auswahl des Dienstleister und der späteren Durchführung wie bei den anderen Sicherheitsprüfungen. Es ist jedoch zu beachten, dass zusätzliche Fragen zu klären sind und damit auch zusätzliche Anforderungen an den Dienstleister gestellt werden müssen.

Zusammenfassend ist besonderes Augenmerk auf folgende Anforderungen zu legen:

- **Kundenanforderungen**
  - Test der produktiven Webanwendung?
  - Spezieller Testzugang (VPN)?
  - mit/ohne IDS/IPS und WAF?
  - Testzeiten
  - ist die Webanwendung automatisch scanbar?
- **Dienstleisteranforderungen**
  - Schutz der Daten und Testergebnisse
  - Zugriff auf die Testergebnisse
  - fachgerechter Support bei der Auswertung der Testergebnisse
  - sind geeignete Scan-Tools vorhanden?

#### 2.1.1.2 Quellcode-Analyse

Eine im Gegensatz zu Penetrationstests weitergehende Aussagekraft bietet eine Quellcode-Analyse. Hierbei wird auf Basis des vollständigen Quellcodes der Webanwendung eine Analyse bzgl. Schwachstellen durchgeführt. Der Quellcode ist allerdings z. B. beim Einsatz einer kommerziellen Webanwendung nicht immer verfügbar.

Aufgrund des meist viele Zeilen umfassenden Codes, ist eine rein manuelle Analyse auch hier nicht mehr möglich. Wichtig bei der Durchführung von Quellcode-Analysen ist die Mächtigkeit der Tools und die Kompetenz der Prüfer, da jedes Tool vielfältig zu parametrisieren ist.

#### 2.1.1.3 Architektur-Analyse

Bei der Architektur-Analyse können viele Parameter der Gesamtumgebung untersucht werden. Ziel hierbei ist es, etwaige bestehende Schwachstellen, – sei es durch den Aufbau der Umgebung, der eingesetzten Serverdienste oder sonstige Zusammenhänge – aufzuzeigen. Mögliche Betrachtungsebenen sind unter Anderem:

- eingesetzte Serverdienste
- Netzverbindungen intern, extern (Internet)
- Verschlüsselung der Daten bei Transport und Speicherung
- Aufbewahrungszeiten von erhobenen Daten
- Ausfallsicherheit von Komponenten

#### 2.1.1.4 Prozess- und Dokumentations-Analyse

Deutlich über die vorgenannten Analysen geht die Prozess- und Dokumentations-Analyse hinaus. Diese umfasst sowohl Vorgaben, als auch Umsetzung von Themenstellungen wie:

- Entwicklervorgaben
- Reaktionsvorgaben

- System- und Serverdienste-Vorgaben (Härtungskonzepte, Administrationsvorgaben, Patch-Management)
- Verschlüsselungsvorgaben (Kryptokonzept)

Viele dieser Fragestellungen werden durch Information-Security-Management-System-Standards (ISMS) behandelt. Im deutschsprachigen Raum setzt sich hier mehr und mehr die *ISO 27001 auf der Basis von IT-Grundschutz* (www.gshb.bund.de), international die *ISO/ECI 27001* durch.

## 2.1.2 Zielformulierung und Umgebungsbeschreibung

### 2.1.2.1 Definition der Testziele

Wie sich aus der Beschreibung der Prüfungsarten ableiten lässt, können Sicherheitsprüfungen von Webanwendungen auf unterschiedliche Testziele abgestimmt werden. Die folgende Matrix stellt die verschiedenen Ausgangslagen und die daraus resultierenden, empfohlenen Prüfungen dar. Die Bewertung erfolgt singulär, d. h. es wird kein aufbauendes Modell verfolgt. Es ist selbstverständlich, dass die Matrix nicht auf jede Umgebung gleich anwendbar ist, sie gibt jedoch einen Eindruck von den entstehenden Aufwänden. In der Matrix wird unterschieden zwischen dem internen Zeitaufwand, der auf Seiten des Kunden für Vorbereitung, Nachbereitung und Mithilfe während der Prüfungen eingeplant werden muss und dem externen Zeitaufwand, der auf Seiten des Dienstleisters entsteht.

| Ziel | Art der Prüfung | Zeitaufwand | |
|---|---|---|---|
| | | intern | extern |
| Bekannte und ausnutzbare Schwachstellen der Webanwendung erkennen | Blackbox-Test | gering | mittel |
| Verlässlicher bekannte und ausnutzbare Schwachstellen der Webanwendung erkennen | Whitebox-Test | mittel | mittel |
| Bekannte und ausnutzbare Schwachstellen der Umgebung erkennen | Blackbox-Test | gering | mittel |
| Verlässlicher bekannte und ausnutzbare Schwachstellen der Umgebung erkennen | Whitebox-Test | mittel | mittel |
| Bekannte und potentielle Schwachstellen der Webanwendung erkennen | Quellcode-Analyse | mittel | hoch |
| Infrastrukturelle Probleme erkennen | Architektur-Analyse | mittel | mittel |
| Probleme im Ablauf und Schwächen in Vorgaben erkennen, ggf. Aufbau eines ISMS | Prozess- und Dokumentations-Analyse | hoch | hoch |

Sofern budgetär nicht alle wünschenswerten Prüfungen durchgeführt werden können, besteht auch die Möglichkeit Worst-Case-Szenarios zu definieren und die Untersuchung auf diese Szenarios zu fokussieren.

### 2.1.2.2 Beschreibung der Umgebung

Um ein einheitliches Verständnis für intern und extern Beteiligte zu ermöglichen, ist es notwendig die zu prüfende Umgebung zu beschreiben. Die folgende Darstellung fokussiert sich primär auf technische Prüfungen der Webanwendung, ohne eine Erweiterung der Prüfungen auf die Umgebung. Es wird empfohlen, folgende Elemente zu beschreiben:

- Überblick der Webanwendung: Aufgabe, unterstützter Geschäftsprozess, Rechte-Management

  Diese Angaben ermöglichen einem bisher nicht mit der Anwendung vertrauten Prüfer eine erste Einschätzung der Aufgabenstellung.

- Zugriffswege: Internet, Intranet, VPN, Proxy

  Insbesondere die Sicherheitsbewertung und die Art der Tests (z. B. bei Einsatz eines Proxys) sind von diesen technischen Faktoren abhängig.

- ggf. spezielle Clients: Fat-Clients, nur spezifische Browser

  Die Einschränkung auf spezifische Clients wirkt sich direkt auf die Testmöglichkeiten aus und erhöht meist den Umfang der Vorbereitungen.

- Logik der Webanwendung: Anzahl der Rechteprofile, Session-Management

  Je nach Anzahl der Rechteprofile erhöhen sich die empfehlenswerten Prüfschritte, um eine Rechteausweitung in den einzelnen Berechtigungsstufen prüfen zu können.

- Beschreibung des Rollenkonzeptes der Benutzer: Welches Authentisierungsverfahren liegt vor bzw. wird genutzt
  - Only Anonymous Users
  - Username/Passwort Authentisierung
  - Username/Passwort mit Selbst-Registrierung, User/Pass/OneTimePass oder Client-Zertifikat

- Umfang und Aufbau der Webanwendung: Anzahl der Seiten/Variablen, verwendete Programmiersprache/Skriptsprache, Datenbanken

  Die Anzahl der Seiten bzw. Variablen ist meist nicht einfach festzustellen und ist auch nur mittelbar ein Indikator für den Prüfumfang. Die Programmiersprache hat Auswirkung auf die anzuwendenden Prüfungen, ebenso die verwendeten Datenbanken und deren Anbindung (z. B. Datenbank auf demselben Host, im selben Netz).

- Funktionsweise der Webanwendung: „klassische“, Controller-/Single-URL-Anwendung

  Die Art und Weise wie der logische Ablauf einer Funktion in der Webanwendung technisch (programmatisch) implementiert ist, ist für den Tester wichtig, da damit die Auswahl der einsetzbaren Tools bestimmt wird und sich erhöhte Testaufwände ergeben. So ist es z. B. schwieriger eine Controller-Anwendung zu untersuchen als eine Anwendung, die für jede Funktionalität eine eigene URL hat.

- Architektur: Netzdiagramm, Serverdienste, Firewall-Systeme (Netz- und Anwendungs-Firewalls)

  Mit Hilfe einer Übersicht der Architektur ist es möglich, technische Fallstricke zu erkennen. So ist z. B. die Frage zu klären, ob die Prüfung unter Einbeziehung der Web Application Firewall erfolgen soll oder nicht. Bezieht man die WAF mit ein, kann eine ggf. unsichere Anwendung durch die WAF als sicher attestiert werden. Sofern die WAF nicht im Fokus steht, sollte daher direkt auf die Webanwendung geprüft werden (die WAF also. gezielt abschalten/deaktivieren oder in der DMZ testen).

- Datenflußdiagramm

  Das Datenflußdiagramm ermöglicht einen raschen Überblick über das Zusammenspiel der einzelnen Komponenten. Erfahrungsgemäß ist die erstmalige Erstellung eines solchen Diagramms bei komplexeren Webanwendungen ein aufwändiges Unterfangen und birgt die eine oder andere Überraschung, da eine solche Gesamtsicht oft fehlt und so intern unterschiedliche Meinungen über die Datenerhebung, -ablage, -weitergabe und -löschung innerhalb einer Webanwendung bestehen.

## 2.1.3 Organisatorische Aspekte

Fast alle Vorhaben in Wirtschaft, öffentlicher Verwaltung, Forschung und Politik werden heute in Form von Projekten verwirklicht. Um die Erfolgsaussichten eines Projektes im Bereich Sicherheitsüberprüfungen von Webanwendungen zu erhöhen werden nachfolgend wichtige Randbedingungen und kritische Faktoren des Projektmanagements erläutert. Der Ablauf eines Projekts zur Sicherheitsüberprüfung von Webanwendungen sei vereinfacht in Abbildung 1 dargestellt.

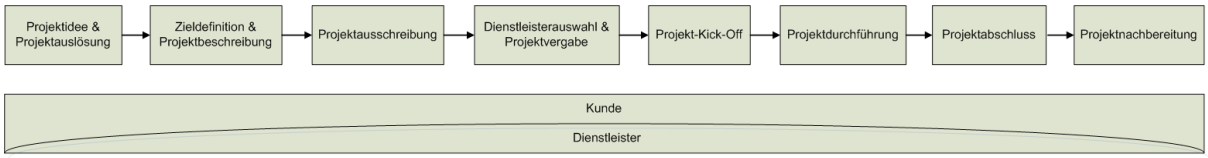


*Abbildung 1: Schematischer Projektablauf für die Sicherheitsüberprüfungen*

### 2.1.3.1 Projektidee und Projektauslösung

Es gibt eine Vielzahl von Gründen für Projekte im IT-Sicherheitsbereich. Für Projekte zur Sicherheitsüberprüfung von Webanwendungen ist das keineswegs anders. Die Projekte werden durch eine Idee, eine Problemstellung, eine Anfrage, eine Compliance-Anforderung, festgestellte Verstöße gegen die Sicherheitsrichtlinie oder ein ungutes Sicherheitsgefühl ausgelöst. In dieser Phase finden auf Seite des Kunden erste Gespräche über Sinn und Nutzen einer Sicherheitsüberprüfung von Webanwendungen statt. Dabei kommen auch nicht selten erste Kontakte zu wichtigen zukünftigen Projektansprechpartnern und Entscheidern zustande.

### 2.1.3.2 Zieldefinition und Projektbeschreibung

In der Vorbereitungsphase des Projektes gilt es Sachziele, Terminziele, Kostenziele und ggf. Sonderzeile zu definieren. Folglich umfasst die Projektvorbereitung auf Kundenseite sowohl inhaltliche als auch organisatorische Aspekte. Im Rahmen der inhaltlichen Projektvorbereitung ist von der Projektleitung die Projektbeschreibung zu erarbeiten. Die inhaltliche Projektbeschreibung umfasst im wesentlichen:

- Ausgangssituation und Begründung: Kompakte Darstellung der Ist-Situation und der Beweggründe für die geplante Sicherheitsüberprüfung der Webanwendung aus Sicht des Kunden.
- Ziele und Meilensteine: Formulierung der Ziele, die der Kunde mit der Realisierung der Sicherheitsüberprüfung erreichen möchte. An dieser Stelle ist zu berücksichtigen, dass sich eine oberflächliche Prüftiefe oder das ausschließliche Prüfen von Testsystemen negativ auf die Qualität und Aussagekraft der Sicherheitsüberprüfung auswirkt. Festlegung der Ergebnisse, die vom Auftraggeber im Rahmen des Projektes erwartet werden und der Meilensteine. So entsteht ein Projektplan und ein Pflichtenheft, in dem die Ziele so exakt definiert werden, dass eine Aufstellung von notwendigen Aufgabenblöcken und benötigten Ressourcen möglich ist.
- Randbedingungen und Abgrenzungen: Formulierung von Aspekten, die bei der Projektdurchführung als Bedingungen und/oder Anforderungen zu beachten sind, beispielsweise: die Verfügbarkeit der Webanwendung und/oder Produktivsysteme die nicht dem Verantwortungsbereich des Kunden unterliegen. Festlegung von Schnittstellen, Datenflüssen, Systemen und Komponenten die zur zu überprüfenden Webanwendung gehören.

Der Dienstleister kann in die Erarbeitung dieser Inhalte eingebunden werden, wenn der Kunde keine eindeutigen Angaben machen kann bzw. diese Lücken, Widersprüche oder Unstimmigkeiten aufweisen. Die organisatorischen Projektvorbereitungen gliedern sich vornehmlich in:

- Teilnehmer: Auf Grund der Projektbeschreibung werden die involvierten Fachbereiche (z. B. Firewall, Netzwerk, System, Datenbank und Anwendung) ausgewählt, die auf Kundenseite an der Erarbeitung der Projektergebnisse wesentlichen Anteil haben. Die ausgewählten Mitarbeiter sind für den Zeitraum der Projektdurchführung frei zustellen. Des weiteren sind Vertretungsregelungen, Eskalationswege und korrespondierende Ansprechpartner involvierter Fachbereiche bekannt zu geben.
- Projektsteuerung und Feedback: Obwohl die Projektsteuerung primär dem Kunden als Auftraggeber obliegt, erweist sich das Einbinden des Dienstleisters meist als vorteilhaft. Insbesondere für die Durchführung der Sicherheitsüberprüfung, also die einzeln aufeinander abgestimmten Aktivitäten und Phasen, sollte die Projektsteuerung an den Dienstleister übertragen werden. Des weiteren sollte an dieser Stelle ein einvernehmliches Vorgehen zur Rückmeldung von Schwachstellen und zum Umgang mit nachträglichen Härtungsmaßnahmen gefunden werden.
- Ort und Zeit: Gemäß dem Projektplan ergeben sich Ort, Zeit und Anforderungen an Ressourcen wie Teilnehmer und Komponenten der Webanwendung.
- Scan-Freigaben: Im Rahmen der inhaltlichen Projektvorbereitung sind die zu untersuchenden Systeme (Test- und/oder Produktivsysteme) und Komponenten festgelegt worden. Um Inkonsistenzen bei den Zielen der technischen Sicherheitsüberprüfung zwischen Kunden, Betreibern (Outsourcing) und Dienstleister zu vermeiden, sollten die Systemverantwortlichen dem Dienstleister konkrete Scan-Freigaben erteilen.
- Vertraulichkeitserklärungen: Mit Hilfe von Vertraulichkeitsvereinbarungen wird der Dienstleister zu Geheimhaltung von Informationen verpflichtet. Die Definition der geheim zu haltenden Informationen obliegt den einzelnen Vertragsparteien. Die Ergebnisse, insbesondere die ermittelten Schwachstellen, sollten geheim zu haltenden Informationen sein.
- Sicherheitsüberprüfungen und -erklärungen: Über die Vertraulichkeitserklärung hinaus regelt das Sicherheitsüberprüfungsgesetz Voraussetzungen und Verfahren zur Sicherheitsüberprüfung von Personen, die mit bestimmten sicherheitsempfindlichen Tätigkeiten betraut werden sollen oder bereits betraut worden sind. Die resultierenden Sicherheitserklärungen sind in drei Ausprägungseigenschaften gegliedert und kommen überwiegend im Behördenbereich zum Einsatz.
- Haftung: Im Vertragsgefüge bzw. den Angeboten der Dienstleister sind meist Haftungskriterien und -beschränkungen formuliert. Die Projektleitung auf Seite des Kunden sollte die Vertragsklauseln prüfen und ggf. vor der Projektvergabe eine Optimierungen des Vertragswerks einfordern.

#### 2.1.3.3 Projektausschreibung

Die Projektausschreibung durch den Kunden oder ggf. durch eine vermittelnde Instanz erfolgt meist nach den branchentypischen Gepflogenheiten des öffentlichen oder privat-wirtschaftlichen Bereichs. In dieser Phase sollte die Kundenseite den potentiellen Dienstleistern unkritische Informationen zur Angebotserstellung zukommen lassen. Neben den inhaltlichen und organisatorischen Aspekten sind für den Dienstleister im Rahmen der Projektausschreibung weiterführende u. A. folgende technische Informationen interessant:

- Allgemeine Kurzbeschreibungen der Systeme bzw. Komponenten
- Vereinfachte Netzwerkpläne
- Vereinfachte Datenflussdiagramme

#### 2.1.3.4 Dienstleisterauswahl und Projektvergabe

Die Phase der Dienstleisterauswahl kann von Kunde zu Kunde grundsätzlich unterschiedlich erfolgen. Um das Projekt möglichst optimal zu vergeben sollten die Angaben der Dienstleister nach Kapitel 2.2 für das konkrete Projekt bewertet und in entsprechender Art und Weise verglichen werden. Das sich eine oberflächliche Prüftiefe negativ auf die Qualität und Aussagekraft der Sicherheitsüberprüfung und positiv auf die Kosten auswirkt und umgekehrt sollte auf Seite des Kunden klar sein.

#### 2.1.3.5 Projekt-Kick-Off

Im Projekt-Kick-Off werden alle Projektinformationen von allen Stellen und Instanzen an die Projektmitarbeiter weitergeleitet. Die Projektinformationen unterscheiden sich im Detaillierungsgrad und sind im Gegensatz zur Projektbeschreibung eher technischer Natur, so dass in dieser Phase dem Dienstleister meist konkrete URLs, IP-Adressen, Hostnamen, angebotene Dienste sowie detaillierte Netzwerkpläne und Datenflussdiagramme bekannt gegeben werden. Der Dienstleister schildert sein Vorgehen und den Umgang mit Rückmeldungen von gefundenen Schwachstellen, zeigt mögliche Risiken auf und weist auf nötige Scan-Freigaben der Systeme und Komponenten hin. Alle Beteiligten stimmen zusammen das Projektvorgehen ab und legen die Arbeitsweise zur Erreichung der Ziele und Meilensteine verbindlich fest. Dabei kann es durchaus zu angepassten Zielen, Meilensteine und Vorgehensweisen gegenüber der durch die Kundenseite geplanten kommen. So werden beispielsweise in Abhängigkeit von Compliance-Anforderungen (z. B. PCI DSS < Version 1.2) Produktivsysteme anstatt Testsysteme einer DoS-Attacke unterzogen, obwohl die Anforderungen an die Verfügbarkeit dies aus geschäftspolitischer Sicht verbietet.

#### 2.1.3.6 Projektdurchführung

Die Projektdurchführung erfolgt in zuvor abgestimmter Zusammenarbeit zwischen Kunde und Dienstleister. Auf der Seite des Kunden sollten dabei die involvierten Mitarbeiter dem Dienstleister die benötigten Zugänge und Berechtigungen nennen und Hintergrundinformationen sowie Rückmeldungen zu bestimmten Angriffsvektoren geben können.

#### 2.1.3.7 Projektabschluss

Nach Erreichung der Ziele und Meilensteine wird ein Projekt zur Sicherheitsüberprüfung von Webanwendungen durch einen Bericht und ggf. einer Präsentation durch den Dienstleister abgeschlossen.

#### 2.1.3.8 Projektnachbereitung

Nach Projektabschluss wird empfohlen die im Bericht getroffenen Einschätzungen intern mit den Verantwortlichen der Fachbereiche zu besprechen und die vorgenommenen Bewertung seitens des Dienstleisters ggf. anzupassen. Von hoher Bedeutung ist die Festlegung von Verantwortlichen zur Behebung der technischen und organisatorischen Schwachstellen.

## 2.2 Dienstleister-Angaben

Die Auswahl eines geeigneten Dienstleisters erweist sich oft als sehr schwierig, da viele Faktoren eine wichtige Rolle spielen und eine echte Vergleichbarkeit der Dienstleister nicht gegeben ist. In diesem Kapitel werden daher unterschiedliche Anforderungen für verpflichtende und optionale Angaben der Dienstleister dargestellt, um dem Kunden die Möglichkeit an die Hand zu geben, verschiedene Dienstleister zu vergleichen.

## 2.2.1 Erforderliche Angaben

### 2.2.1.1 Unternehmensgeschichte – Alter, Spezialisierung

Die Unternehmensbeschreibung und die Darstellung der Unternehmensgeschichte dient der Einschätzung der fachlichen Qualifikation eines Unternehmens. Relevante Angaben sind unter anderem die Beschreibung der Entstehung und der Aufbau des Unternehmens sowie ein Dienstleistungsportfolio, das darstellt, welche Aspekte der IT-Sicherheit vom Unternehmen bedient werden. Des Weiteren ist es wichtig, dass der Dienstleister einen Überblick über seine bisherige Erfahrung in den behandelten Themenbereichen vorstellt.

Die Beschreibung und die Geschichte eines Unternehmens können bereits einige Anhaltspunkte für den Auftraggeber bieten, sind jedoch nicht zwingend ein Merkmal für die Qualität des Dienstleisters.

Aus der Beschreibung sollte eine konkrete Spezialisierung auf das Thema Webanwendungssicherheit sowie Erfahrung auf diesem Gebiet eindeutig hervorgehen. Wird etwa das Thema Webanwendungssicherheit in der Beschreibung gar nicht erwähnt, lässt dies darauf schließen, dass die Komplexität des Themas unterschätzt und Untersuchungen nur sehr oberflächlich durchgeführt werden. Der Dienstleister sollte für das Thema ein dediziertes Team haben, das sich aus mehreren Mitarbeitern zusammensetzt. Nur dadurch kann ein Erfahrungs- und Wissensaustausch sowie eine Qualitätssicherung innerhalb des Teams erreicht werden. Bei einem Ein-Mann-Team ist außerdem zu bedenken, dass ein unerwarteter Ausfall des Mitarbeiters den Projekterfolg gefährden kann.

Prinzipiell sollte der Dienstleister bereits mehrjährige Erfahrung im Themengebiet Webanwendungssicherheit haben. Wurde das Unternehmen allerdings neu gegründet oder das Thema erst kürzlich aufgegriffen, so kann auch die Erfahrung und Qualifizierung einzelner Mitarbeiter Rückschlüsse auf die Qualität des Dienstleisters geben.

Enthält die Unternehmensbeschreibung auch Hinweise auf Veröffentlichungen, Mitgliedschaften in Fachorganisationen oder Zertifizierungen des Unternehmens, ist dies ein Pluspunkt.

Aufgrund der entstehenden Kosten halten sich manche Unternehmen hier aber auch absichtlich zurück. Aus diesem Grund sollten diese Aktivitäten nicht vorausgesetzt werden und werden daher in Abschnitt 2.2.2 „Optionale Angaben, weiche Faktoren“ genauer erläutert.

### 2.2.1.2 Qualifizierung der designierten Projektmitarbeiter (Projektteam)

Der Erfolg eines Projektes hängt maßgeblich von der Qualifikation und der Erfahrung der einzelnen Projektmitarbeiter ab. Daher ist es besonders wichtig, dass der Dienstleister für das Projekt jene Mitarbeiter bereitstellen kann, welche den Anforderungen der zu überprüfenden Webanwendung am besten entsprechen.

Der Dienstleister soll für jeden am Projekt beteiligten Mitarbeiter ein Profil vorlegen, welches die Qualifikation des Mitarbeiters widerspiegelt. Ein solches Profil sollte die folgenden Punkte beinhalten:

- Ausbildung

  Die Schilderung des Ausbildungsweges soll dazu dienen, einen ersten Eindruck vom Mitarbeiter zu gewinnen. Sie sagt noch nichts über die Eignung des Mitarbeiters für das Projekt aus.

- Projekterfahrung

  Diese Beschreibung sollte die Projekterfahrung in Jahren, sowie die Anzahl, die Dauer und den Typ (Quellode-Analyse/Penetrationstest) der Projekte enthalten. Sie kann Auskunft darüber geben, ob der Mitarbeiter bereits Erfahrungen aus früheren

Projekten gesammelt hat, die der Kunde für die zu untersuchende Webanwendung benötigt.

- Spezialisierung

  Hier sollte der Dienstleister auf die besonderen Fähigkeiten und Kenntnisse eines Mitarbeiters eingehen, wie z. B. bestimmte Technologien oder Programmiersprachen. Diese Informationen geben – wie die Projekterfahrungen – Aufschluss darüber, ob ein Mitarbeiter für das Projekt grundsätzlich oder gar besonders geeignet ist.

- Zertifizierung

  Der Dienstleister sollte hier – soweit vorhanden – die Zertifizierungen des Mitarbeiters benennen. Es sei darauf hingewiesen, dass den Autoren zum Zeitpunkt des Entstehens dieses Papers keine speziellen Zertifizierungen im Umfeld der Webanwendungssicherheit bekannt waren.

Neben beteiligten Mitarbeitern sollte der Dienstleister zumindest einen weiteren Mitarbeiter benennen können, der beim Ausfall eines für das Projekt zugeteilten Mitarbeiters dessen Rolle übernehmen kann.

#### 2.2.1.3 Darstellung der Methoden und Vorgehensweise im Projekt

Die Darstellung der projektspezifischen Vorgehensweise und Untersuchungsmethodik des Dienstleisters soll sicherstellen, dass der Dienstleister überhaupt ein strukturiertes Vorgehen hat, das von Seiten des Kunden nachvollziehbar ist und eingeplant werden kann. Eine strukturierte Untersuchungsmethodik soll dafür sorgen, dass die Ergebnisse der Sicherheitsuntersuchung nachvollziehbar sind.

In diesem Punkt sollte der Dienstleister darlegen, wie er sich den Ablauf innerhalb des Projektes vorstellt. Ein Beispielvorgehen in einem einfachen Projekt könnte etwa folgendermaßen aussehen:

- Kick-Off-Meeting beim Kunden
- Dokumenten-Review (bei Whitebox-Tests)
- Praktische Webanwendungsuntersuchung
- Berichterstellung
- Präsentation der Ergebnisse beim Kunden

Wichtig ist hier, dass der Dienstleister die einzelnen Phasen bereits mit Aufwandsabschätzungen und konkreten Meilensteinen hinterlegt. Pro Phase sollte außerdem definiert sein, welche Informationen vom Kunden notwendig sind, und welche Ergebnisse (z. B. Abschlussbericht) der Dienstleister liefert. Nur so kann auch der Kunde notwendige Ressourcen für das Projekt einplanen und die zeitgerechte Durchführung der Untersuchung überwachen.

Des Weiteren sollte der Dienstleister für den Punkt „Webanwendungsuntersuchung“ eine genaue Methodik vorstellen, die einen Einblick gibt, wie die Tester bei ihrer Untersuchung vorgehen. Die genaue Methodik wird sich von Dienstleister zu Dienstleister unterscheiden. Wichtig ist die Analyse durch den Kunden, ob der Dienstleister seine Vorgehensweise bereits an die Vorgaben des Kunden angepasst hat und dadurch bereits in der Angebotsphase eine kundenorientierte Haltung einnehmen konnte. Typischerweise enthält die Vorgehensweise folgende Komponenten

- Automatisierte Tests

  Mit Hilfe von kommerziellen, frei verfügbaren oder selbst entwickelten Scan-Tools können Webseiten und Webanwendungen automatisiert überprüft werden. Solche Tools können vor allem bekannte Schwachstellen in bekannten Anwendungen, einfache Anwendungsprobleme sowie Schwachstellen in Server-Software identifizieren. Automatisierte Tests können bereits in sehr kurzer Zeit auch

komplexere Anwendungen abdecken und zumindest einen ersten Eindruck über den Sicherheitszustand einer Anwendung geben.

- Manuelle Tests

  Führt ein Dienstleister automatisierte Scans durch, so werden häufig die gefundenen Schwachstellen noch einmal manuell überprüft, um False-Positives zu vermeiden. Zusätzlich dazu können weitere manuelle Tests durchgeführt werden, die auf vordefinierten und generischen „Test-Cases“ basieren oder vollständig auf der Kreativität des einzelnen Testers beruhen. Ein Dienstleister kann beispielsweise eine Liste von generischen Test-Cases (Test-Suite) besitzen, aus der die abzuarbeitenden Test-Cases je nach Aufbau und Zusammensetzung der Anwendung ausgewählt werden. Während die Ergebnisse bei Verwendung einer Test-Suite auch unter verschiedenen Testern sehr vergleichbar sein sollten, hängt die Qualität der Ergebnisse bei kreativem Testen sehr stark von den Kenntnissen und der Erfahrung des einzelnen Testers ab.

Nur aufgrund der Beschreibung der Untersuchungsmethodik auf die Qualität der Untersuchungsergebnisse zu schließen, ist unmöglich. Einige wichtige Punkte sollten bei der Beurteilung allerdings berücksichtigt werden. Aufgrund der hohen Komplexität und Individualität der meisten Webanwendungen können mit automatisierten und generischen Tests nur sehr beschränkte Ergebnisse erzielt werden. Sämtliche Sicherheitsprobleme, die sich aus der individuellen Programmierung der Anwendung oder aus Problemen in der Anwendungslogik ergeben, können nur mit Hilfe von kreativen Tests, die auf die spezifische Anwendung eingehen, identifiziert werden.

Daher sollte ein Webanwendungstest auf jeden Fall auch eine ausgeprägte kreative Komponente enthalten. Basis dafür sind automatisierte Scans und/oder vordefinierte Testfälle, welche eine systematische Überprüfung oberflächlicher Schwachstellen mit hoher Abdeckung ermöglichen. Werden automatisierte Scans durchgeführt, darf auf keinen Fall eine manuelle Verifikation der Ergebnisse zur Eliminierung von False-Positives fehlen. Da bei der kreativen Komponente vor allem das Wissen und die Erfahrung des Testers für die Qualität ausschlaggebend sind, muss für eine Bewertung verschiedener Dienstleister hier auf Merkmale wie Qualifikation und Erfahrung der Projektmitarbeiter, genereller Eindruck des Unternehmens und bisherige Referenzen des Unternehmens zurückgegriffen werden.

Sowohl die Beschreibung der Vorgehensweise als auch der Untersuchungsmethodik sollte im Angebot nicht nur generisch aufgeführt, sondern bereits individuell an den Kunden angepasst sein. Basierend auf der jeweils zu testenden Anwendung, sollte der Dienstleister auch die eingesetzten Werkzeuge und Scan-Tools auflisten und kurz beschreiben.

#### 2.2.1.4 Darstellung der Projektergebnisse

Zur Behebung und Weiterbehandlung der gefundenen Sicherheitsschwachstellen ist es für den Kunden wesentlich, in welcher Form und Qualität die Ergebnisse der Sicherheitsuntersuchung durch den Dienstleister dokumentiert werden. Daher ist es wichtig, dass der Kunde bereits vor seiner Entscheidung für einen Dienstleister einen Eindruck darüber bekommt, wie der Dienstleister seine Ergebnisse darstellt und bewertet.

Zu diesem Zweck sollte der Dienstleister bereits in seinem Angebot eine Gliederungsübersicht des späteren Berichts sowie eine Beschreibung seiner Bewertungsmethode mitliefern. Die Gliederung des Berichtes sollte auf jeden Fall folgende Komponenten enthalten:

- Executive Summary

  Die Ergebnisse und Erkenntnisse der Untersuchung sollten auf einer Seite kurz und prägnant zusammengefasst sein.

- Zusammenfassung der Schwachstellen

Die Anzahl, Art und Schwere der gefundenen Schwachstellen sollte an einer zentralen Stelle überschaubar sein.

- Inhaltsverzeichnis
- Um im Bericht zügig navigieren zu können, muss ein Inhaltsverzeichnis mit Seitenangaben vorhanden sein.
- Ausführliche Beschreibung der Schwachstellen

  Für eine effiziente Beseitigung der Sicherheitsprobleme ist eine detaillierte Beschreibung der Schwachstellen notwendig. Diese sollte eine Kurzbeschreibung, die Auswirkung der Schwachstelle, eine Risikoeinschätzung, Referenzen und ggf. die genaue Vorgehensweise zur Ausnutzung der Schwachstelle beschreiben. Dies ist notwendig, damit ein Angriff durch den Kunden oder Anwendungsentwickler nachvollzogen und reproduziert werden kann.

Um sich ein genaues Bild über den tatsächlichen Bericht machen zu können, sollte der Dienstleister idealerweise einen Beispielreport zur Verfügung stellen. Wichtig für die Bewertung eines solchen Beispielberichts ist, dass die detaillierte Beschreibung und Bewertung (z. B. Schadenshöhe und Ausnutzbarkeit) der Sicherheitsprobleme individuell auf das Einsatzszenario des Kunden angepasst ist und nicht nur Tool-generierte Ergebnisse oder generische Bewertungen erhält. Eine Schwachstelle kann beispielsweise als weniger kritisch eingestuft werden, wenn sie lediglich von sehr wenigen vertrauenswürdigen Benutzern ausgenutzt werden kann. Viel kritischer ist dieselbe Schwachstelle, wenn sie für anonyme Benutzer aus dem gesamten Internet zugänglich ist.

Der Dienstleister sollte des weiteren darlegen, nach welcher Methode oder Klassifizierung er die gefundenen Schwachstellen bewertet. Hier verwenden Dienstleister häufig sehr granulare und detaillierte Bewertungen auf beliebigen Skalen (z. B. 3, 10 oder 100). Hierbei sollte allerdings im Auge behalten werden, dass ein Webanwendungstest keine Risikoanalyse ersetzen kann. Für eine Risikoanalyse sind detaillierte Angaben des Kunden notwendig, um genaue Bewertungen der Wahrscheinlichkeit und Schadenshöhe von Schwachstellen vornehmen zu können. Diese Informationen liegen häufig in einer Sicherheitsuntersuchung nicht vor. Es ist zwar wichtig, offensichtliche Rahmenbedingungen des Kunden (z. B. sehr eingeschränkter Zugriff auf unsichere Funktionalität) in die Bewertung einfließen zu lassen, allerdings kann ein Tester der Webanwendung ohne detaillierte Kenntnisse des Einsatzszenarios und der Prozesszusammenhänge in der Regel zum Beispiel keine Unterscheidung zwischen einer Eintrittswahrscheinlichkeit von 6 oder 7 (auf einer Skala von 10) treffen. Sinnvoll sind daher eher grobe Einordnungen in Sicherheitsstufen wie etwa „Hoch“, „Mittel“, „Niedrig“ oder „Informativ“.

#### 2.2.1.5 Zusammensetzung des Preises

Im Angebot sollte der Dienstleister seinen Preis auf genaue Arbeitspakete aufschlüsseln. Nur so wird für den Kunden transparent, wie sich der Preis für die Sicherheitsuntersuchung zusammensetzt und wie etwa die Arbeitsschwerpunkte bei unterschiedlichen Dienstleistern gesetzt werden.

### 2.2.2 Optionale Angaben, weiche Faktoren

Neben den erforderlichen Angaben zum Unternehmen, der Qualifikation der Projektmitarbeiter und der Vorgehensweisen im Projekt sind auch weitere optionale Angaben von Interesse, um über die Eignung eines Dienstleisters zu entscheiden. Zu diesen zählen z. B. die Referenzen oder Referenzprojekte des Dienstleisters, seine Veröffentlichungen oder seine Mitgliedschaften bei anerkannten Organisationen.

#### 2.2.2.1 Referenzen/Referenzprojekte

Referenzen und/oder Referenzprojekte können ein Hinweis darauf sein, dass andere Kunden mit dem Dienstleister zufrieden waren. Der Kunde darf sich aber nicht auf die

reine Aufzählung der Referenzen oder den „großen Namen“ in den Referenzen verlassen. Erst eine persönliche Befragung der Referenzpersonen zu ihrer Zufriedenheit hinsichtlich der Projektergebnisse, der Vorgehensweise oder auch der Qualifikation der Mitarbeiter kann entscheidende Argumente für oder wider den Dienstleister liefern. Der Kunde sollte aber auch verstehen, dass der Dienstleister in manchen Fällen aus Diskretionsgründen keine Referenzen nennen kann bzw. darf. Hier könnte es sich beispielsweise um Unternehmen handelt, die in einem sensiblen Umfeld agieren (Behörden, Militär, Finanzdienstleister).

#### 2.2.2.2 Veröffentlichungen

Falls der Dienstleister Veröffentlichungen, wie z. B. Fachartikel oder Security-Advisories, oder auch Vorträge auf bekannten Sicherheitsveranstaltungen vorweisen kann, sollten diese auch mitsamt einer kurzen Beschreibung angegeben werden. Der Kunde hat dadurch die Möglichkeit, die Themen kennenzulernen, mit denen sich der Dienstleister befasst, und kann so dessen Eignung für das Projekt besser beurteilen.

#### 2.2.2.3 Mitgliedschaften

Die Mitgliedschaften des Dienstleisters bei IT-sicherheitsrelevanten Organisationen sollten genannt werden. Dabei sollte der Dienstleister unbedingt angeben, ob es sich um eine passive oder aktive Mitgliedschaft handelt. Eine aktive Mitgliedschaft kann auf eine Anerkennung der Expertise des Dienstleisters und seine Vorreiterrolle in dem respektiven Bereich hindeuten.

#### 2.2.2.4 Zertifizierungen des Unternehmens

Der Dienstleister sollte relevante Zertifizierungen (z. B. *ISO/IEC 27001* oder *ISO 9001*) seines Unternehmens nennen. Diese können ein Hinweis für ein dokumentiertes, methodisches Vorgehen bedeuten.

#### 2.2.2.5 Umgang mit Daten

Es muss sichergestellt sein, dass der Austausch und die Speicherung von Dokumenten, die potentiell sensible Informationen enthalten (z. B. Quellcode, interne Dokumente des Kunden, Ergebnisse aus der Sicherheitsuntersuchung usw.), verschlüsselt erfolgt. Der Dienstleister sollte daher angeben, über welche Möglichkeiten der sicheren Kommunikation, Übertragung und Speicherung von Daten er verfügt. Der Kunde sollte überprüfen, ob die angebotenen Lösungen mit seinen eigenen kompatibel sind bzw. von ihm genutzt werden können.

#### 2.2.2.6 Verfügbarkeit einer Haftpflichtversicherung

Der Dienstleister soll angeben, ob eine Haftpflichtversicherung vorhanden und in welcher Höhe diese abgeschlossen ist. Insbesondere gilt das für Projekte, bei denen Schadenersatzansprüche entstehen können. Dies kann z. B. bei Überprüfung von Produktivanwendungen der Fall sein, bei denen ein Ausfall oder eine fehlerhafte Manipulation von Daten aufgrund der Fahrlässigkeit der Penetrationstester Kosten nach sich ziehen . Solcherlei Kosten wären durch eine entsprechende Haftpflichtversicherung abgedeckt.

# A Anhang

## A.1 Referenzen

http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf
*BSI* Bundesamts für Sicherheit in der Informationstechnik: *Durchführungskozept für Penetrationstests*

http://www.gshb.bund.de
BSI: *IT-Grundschutz Handbuch*

http://www.osstmm.org/
ISECOM: *Open Source Security Testing Methodology Manual*

http://www.owasp.org/index.php/Category:OWASP_Testing_Project
OWASP: *Testing Guide*

http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
OWASP: *Application Security Verification Standard*

http://www.owasp.org/index.php/Category:Attack
OWASP Category:Attack

http://www.owasp.org/index.php/Category:Threat
OWASP Category:Threat

http://www.owasp.org/index.php/Category:Vulnerability
OWASP Category:Vulnerability

http://projects.webappsec.org/Threat-Classification-Reference-Grid
WASC Web Application Security Consortium: WASC Threat Classification

http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.de.pdf
WASTC Web Application Security Consortium: Web Security Threat Classification

http://www.gesetze-im-internet.de/s_g/index.html
Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes

## A.2 Checkliste: Anforderungen Kundenseite

| | Anforderung | Bemerkung / Kommentar |
|---|---|---|
| **Art der Prüfung** | | |
| O | Vulnerability-Assessment (VA) / Penetrationstest der Webanwendung<br>Blackbox, Whitebox, Denial-of-Service | |
| O | Quellcode-Analyse<br>Automatisierte/Manuelle Überprüfung | |
| O | Architektur-Analyse<br>Eingesetzte Serverdienste, Netzverbindungen, Verschlüsselung der Daten, Ausfallssicherheit | |
| O | Prozess- und Dokumentations-Analyse<br>ISMS, Regelwerke, Vorgaben/Guidelines | |
| **Zielformulierung und Umgebungsbeschreibung** | | |
| O | Definition der Testziele<br>Art der Prüfung, Worst-Case-Szenarien | |
| O | Beschreibung der Umgebung<br>Überblick der Webanwendung, Zugriffswege, Logik, Rollenkonzept, Umfang und Aufbau, Funktionsweise, Architektur, Datenfluss | |
| **Organisatorische Aspekte** | | |
| O | Projektidee und Projektauslösung<br>Problemstellung, Anforderung, Sinnhaftigkeit, Nutzen | |
| O | Zieldefinition und Projektbeschreibung<br>Ausgangssituation, Ziele und Meilensteine, Randbedingungen und Abgrenzung, Teilnehmer, Projektsteuerung und Feedback, Ort und Zeit, Scan-Freigaben, Vertraulichkeitserklärung, Sicherheitsüberprüfung von Personen, Haftung | |
| O | Projektausschreibung<br>Informationen zur Angebotserstellung, grober technischer Überblick | |
| O | Dienstleisterauswahl und Projektvergabe<br>Vorgang, zeitlicher Rahmen, Kommunikation | |
| O | Projekt-Kick-Off<br>Technische Details (URLs, IP-Adressen, Hostnamen, Netzwerkpläne, Datenflussdiagramme, Testsysteme/Produktivsysteme), Vorgehensweise | |
| O | Projektdurchführung<br>Involvierte Mitarbeiter, Berechtigungen, Abstimmung Angriffsvektoren | |
| O | Projektabschluss<br>Bericht, Präsentation | |
| O | Projektnachbereitung<br>Abstimmung Bewertung der Schwachstellen und Gegenmaßnahmen, Verantwortlichkeiten | |

## A.3 Checkliste: Anforderungen Dienstleister-Angaben

| | Anforderung | Bemerkung / Kommentar |
|---|---|---|
| **Erforderliche Angaben** | | |
| O | Unternehmensgeschichte – Alter, Spezialisierung<br>Entstehung, Dienstleistungsportfolio, Erfahrung, Spezialisierung Webanwendungssicherheit | |
| O | Qualifizierung der designierten Projektmitarbeiter (Projektteam)<br>Ausbildung, Projekterfahrung, Spezialisierung, Zertifizierung, Möglichkeit Ersatz-Projektmitarbeiter | |
| O | Darstellung der Methoden und Vorgehensweise im Projekt<br>Ablauf des Projekts, Beschreibung Projektphasen, Methodik der Untersuchung (automatisierte/manuelle Tests, kreative Komponente) | |
| O | Darstellung der Projektergebnisse<br>Beispielbericht, Klassifizierung der Schwachstellen | |
| O | Zusammensetzung des Preises<br>Aufschlüsselung in Arbeitspakete, Transparenz | |
| **Optionale Angaben, weiche Faktoren** | | |
| O | Referenzen/Referenzprojekte<br>Projektumfang, Art des Projekts, Befragung Referenzpersonen | |
| O | Veröffentlichungen<br>Fachartikel, Vorträge, Beschreibung des Inhalts | |
| O | Mitgliedschaften<br>Aktive/Passive Mitgliedschaft, Rolle, Aufgaben | |
| O | Zertifizierungen des Unternehmens<br>Art und Umfang der Zertifizierung, Gültigkeit | |
| O | Umgang mit Daten<br>Verschlüsselung (Übertragung, Speicherung) | |
| O | Verfügbarkeit einer Haftpflichtversicherung<br>Versicherungsbetrag, Abdeckung | |