Bundesamt
für Sicherheit in der
Informationstechnik

Studie

Durchführungskonzept für

Penetrationstests

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung und Zielsetzung der Studie ... 4

1.1 Einführung in die Thematik ... 4

1.2 Vorgehen und Aufbau der Studie ... 4

2 IT-Sicherheit und Penetrationstests ... 5

2.1 Bedrohungen ... 6

2.2 IT-Sicherheitsmaßnahmen ... 8

2.3 Entwicklung von Penetrationstests ... 8

2.4 Vorgehensweise für Penetrationstests ... 8

3 Einordnung und Zielsetzung von Penetrationstests ... 9

3.1 Ansatzpunkte und Zugangswege für Penetrationstests ... 9

3.2 Zielsetzungen von Penetrationstests ... 10

3.3 Grenzen von Penetrationstests ... 12

3.4 Klassifikation ... 12

3.5 Mehrstufiges Vorgehen ... 17

4 Rechtliche Überlegungen ... 18

4.1 Gesetzliche Vorschriften als Motivation für Penetrationstests ... 18

4.2 Bei der Durchführung von Penetrationstests zu beachtende gesetzliche Rahmenbedingungen ... 27

4.3 Wesentliche Vertragsbedingungen für das Auftragsverhältnis zwischen Penetrationstester und Auftraggeber ... 30

5 Rahmenbedingungen ... 36

5.1 Organisatorische Voraussetzungen ... 36

5.2 Personelle Voraussetzungen ... 39

5.3 Technische Voraussetzungen ... 41

5.4 Ethische Überlegungen ... 42

6 Methodik für die Durchführung von Penetrationstests ... 44

6.1 Anforderungen an eine Methodik für die Durchführung von Penetrationstests ... 44

6.2 Die fünf Phasen eines Penetrationstests ... 45

6.3 Vorgehensweise ... 47

6.4 Module für die Prüfungshandlungen ... 48

6.5 Modulbeschreibungen ... 53

6.6 Dokumentation des Penetrationstests ... 99

7 Durchführung von Penetrationstests ... 100

7.1 Vorbereitung ... 100

7.2 Informationsbeschaffung ... 102

7.3 Bewertung der Informationen / Risikoanalyse ... 103

7.4 Aktive Eindringversuche ... 104

7.5 Abschlussanalyse / Nacharbeiten / Clean-up ... 105

Glossar ... 107

Literaturverzeichnis ... 111

Anhang ... 113

A.1 OSSTMM ... 113

A.2 NIST Guideline on Network Security Testing ... 114

A.3 ISACA Switzerland – Sicherheitsüberprüfung von IT-Systemen mit Hilfe von Tiger Teams ... 114

A.4 Zertifikationen im Bereich Penetrationstests ... 116

A.5 Zuordnung der I- und E-Module zu den Modulen des OSSTMMs ... 121

A.6 Checklisten und Vorlagen zur Dokumentation ... 125

A.7 Tools ... 132

1 Einleitung und Zielsetzung der Studie

Die vorliegende Studie „Durchführungskonzept für Penetrationstests“ beschäftigt sich mit dem Einsatz von Penetrationstests in sicherheitsrelevanten IT-Systemen. Die Sicherheit jener Systeme, die über Verbindungen zu öffentlichen Netzen verfügen, unterliegen in besonderer Weise unautorisierten, meist anonymen Zugriffsversuchen. In dieser Situation werden Testmethoden benötigt, die sich des Blickwinkels der Angreifer bedienen, um möglichst reale Testbedingungen schaffen zu können.

Im technischen Sprachgebrauch versteht man unter einem Penetrationstest den kontrollierten Versuch, von „außen“ in ein bestimmtes Computersystem bzw. -netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden die gleichen bzw. ähnliche Techniken eingesetzt, die auch bei einem realen Angriff verwendet werden. Die hierbei identifizierten Schwachstellen können dann durch entsprechende Maßnahmen behoben werden, bevor diese von unautorisierten Dritten genutzt werden können.

Die Studie richtet an Unternehmen und Einrichtungen, die Penetrationstests anbieten bzw. in Zukunft anbieten wollen. Es wird eine strukturierte Vorgehensweise für Penetrationstests dargestellt, die eine effiziente und zielgerichtete Durchführung der Tests erleichtert bzw. sicherstellen kann. Eine weitere Zielgruppe sind Entscheider in Unternehmen und öffentlichen Einrichtungen, die einen Penetrationstest beauftragen möchtenum Hilfestellung für Auswahlkriterien zu erhalten.

Die Studie stellt keine Anleitung zum „Hacken“ von Netzen und Systemen dar, daher wurde bewusst auf detaillierte technische Anleitungen und Beschreibung von Werkzeugen, die in Penetrationstests verwendet werden, verzichtet.

1.1 Einführung in die Thematik

Bei der Nutzung öffentlicher Netzstrukturen sehen sich Unternehmen und öffentliche Einrichtungen vielfältigen Gefährdungen gegenüber. Es sind komplexe Kommunikationsstrukturen entstanden, die sich oftmals den einzelnen Einrichtungen bzw. Unternehmen nicht mehr ganzheitlich erschließen und auf die teilweise nur unwesentlich oder überhaupt nicht Einfluss genommen werden kann. Unternehmen und öffentliche Einrichtungen schließen sich an das Internet an und geben damit einen Teil ihrer Verantwortung (z. B. Verfügbarkeit fremder Server und Netze) ab, ebenso setzen sie sich damit neuen Bedrohungen aus, auf die angemessen reagiert werden muss.

1.2 Vorgehen und Aufbau der Studie

Der Aufbau der Studie folgt einer Ablaufchronologie von der Auftragsanfrage bis zum Testabschluss, einschließlich der zu erstellenden Dokumentation. Dadurch bedingt erfolgt die Darstellung der eigent-

lichen Methode und deren Anwendung am Ende der Studie. So kann der Leser sich durch einen definierten Ablauf führen lassen oder auch nur die für ihn interessanten Kapitel auswählen.

Eine bestimmte Reihenfolge ist für das Verständnis keine zwingende Voraussetzung – entsprechendes Fachwissen vorausgesetzt.

Im ersten Kapitel dieser Studie wird eine allgemeine Einführung in die Thematik der Penetrationstests gegeben. Dazu gehört eine Definition der Zielgruppen und eine Schilderung des Aufbaus dieser Studie. Für interessierte Leser ist im zweiten Kapitel eine kurze Darstellung der Grundlagen der IT-Sicherheit enthalten.

Das dritte Kapitel versucht die Thematik „Penetrationstests“ anhand von Zielsetzungen („welche Ziele können mit Penetrationstests erreicht werden?“), Abgrenzungen („was unterscheidet einen Penetrationstest von einer Revision bzw. Prüfung?“) und von Klassifikationen („welche Kriterien sollte ein Penetrationstest erfüllen?“) in die Test- und Prüfungssystematik einzuordnen.

Anschließend folgen im vierten Kapitel rechtliche Überlegungen, die den Fokus weniger auf den strafrechtlichen Aspekt legen als auf den zivilrechtlichen.

Die Rahmenbedingungen mit den organisatorischen, personellen und technischen Anforderungen werden im fünften Kapitel behandelt. Besonderer Wert wurde auf die „ethischen“ Überlegungen gelegt, um die Grenzen eines Penetrationstests und insbesondere die Verhältnismäßigkeit der Mittel deutlich zu machen.

Nachdem alle Voraussetzungen für Penetrationstests nachvollziehbar erarbeitet wurden, wird anschließend deren Methodik sowie deren Dokumentation ausführlich beschrieben.

Zum besseren Verständnis wird die Umsetzung der Methode anhand des siebten Kapitels „Durchführung von Penetrationstests“ erläutert. Damit soll der Leser durch die Anwendung der einzelnen Methodenschritte geführt werden, um die Verwendung in der Verwaltung bzw. dem Unternehmen zu erleichtern und damit die Praxisnähe noch einmal zu betonen.

Informationen, die zwar von Interesse sind, aber nicht direkt zum Thema gehören, sind im Anhang zu finden. Der Leser erhält Informationen zu Zertifikaten für Penetrationstests, weitere Informationen zur Methodik und Vorschläge für zu verwendende Formblätter.

2 IT-Sicherheit und Penetrationstests

Durch einen Penetrationstest kann geprüft werden, inwieweit die Sicherheit der IT-Systeme durch Bedrohungen von Hackern, Crackern, etc. gefährdet ist bzw. ob die IT-Sicherheit durch die eingesetzten Sicherheitsmaßnahmen aktuell gewährleistet ist. Um die Bedrohungen der IT-Sicherheit einordnen zu können, wird in diesem Kapitel zunächst eine Übersicht der existierenden Bedrohungen gegeben. Dabei werden die häufigsten Täterprofile dargestellt und verbreitete Angriffstechniken auf IT-Systeme

geschildert. Daran schließt sich eine kurze Übersicht der üblicherweise eingesetzten IT-Sicherheitsmaßnahmen an, die teilweise durch Penetrationstests geprüft werden können. Es folgt eine Darstellung der Entwicklung von Penetrationstests.

2.1 Bedrohungen

Aus einer gemeinsamen Studie des US-amerikanischen Computer Security Institute's CSI und des FBI's [CSI02, S.11] geht hervor, dass befragten Unternehmen im Jahr 2001 ein durchschnittlicher finanzieller Verlust von 4,5 Mio. US$ durch Informationsdiebstahl aufgrund von Computerkriminalität entstanden ist. Unterschiedliche Motivationen können für Täter ausschlaggebend sein, Angriffe auf IT-Infrastrukturen durchzuführen. Im Folgenden werden die wichtigsten Tätergruppen und deren Motivation dargelegt.

2.1.1 Täterprofile

Üblicherweise wird in der medialen Berichterstattung unter dem Begriff „Hacker“ pauschal eine Person bezeichnet, die unbefugt in fremde IT-Systeme eindringt. Oftmals wird jedoch zwischen „Hackern“, „Crackern“ und „Script Kiddies“ unterschieden. Während „Hacker“ dabei als experimentierfreudige Programmierer angesehen werden, die sich aus technischem Interesse mit Sicherheitslücken in IT-Systemen auseinander setzen, werden unter „Crackern“ Personen verstanden, die sich aufgrund krimineller Energie der Schwachstellen von IT-Systemen bedienen, um dadurch rechtswidrige Vorteile oder gesellschaftliche Aufmerksamkeit bzw. Anerkennung zu erlangen.

Bei „Script Kiddies“ handelt es sich meist um Täter, die ohne umfangreiches Hintergrundwissen und aus Neugier weitestgehend vorgefertigte Angriffstools aus dem Internet gegen willkürlich ausgewählte oder besonders exponierte Ziele anwenden.

Cracker, die über privilegiertes Wissen über die Organisation verfügen, die sie angreifen wollen, werden als Insider bezeichnet. Oft handelt es sich bei Insidern um frustrierte (ehemalige) Mitarbeiter einer Organisation, die ihr erworbenes Wissen über betriebsinterne Sachverhalte dazu nutzen, der Organisation Schaden zuzufügen. Die Gefahr, die von Insidern ausgeht, ist dabei als besonders hoch einzuschätzen, da sie mit der technischen und organisatorischen Infrastruktur vertraut sind und vorhandene Schwachstellen möglicherweise bereits kennen.

Neben den oben beschriebenen Tätergruppen stellt auch die Wirtschaftsspionage eine ernst zu nehmende Bedrohung dar: Ziel der Wirtschaftsspionage ist es, von Betriebsgeheimnissen wie innovativen technischen Konzepten, Strategien und Ideen, die einen Wettbewerbsvorteil bedeuten, Kenntnis zu erlangen und zum eigenen Vorteil zu verwenden.

2.1.2 Vorgehensweisen

Es existieren mehrere Möglichkeiten, IT-Systeme in ihrer Funktionsweise zu manipulieren oder zu schädigen bzw. einen Angriff auf IT-Systeme vorzubereiten.

- Angriffe über das Netzwerk

  Unter „Angriffe über das Netzwerk“ versteht man Attacken, die unter der Nutzung von Funktionalitäten der eingesetzten Netzwerkprotokolle auf Netzwerkkomponenten, Computersysteme und oder Applikationen stattfinden. Diese Art von Angriffen macht sich Schwachstellen oder Unzulänglichkeiten in Hard- und Software zu nutze, um Angriffe vorzubereiten oder durchzuführen.

  Mögliche Arten von Angriffen über das Netzwerk sind Portscanning, IP-Spoofing, Sniffing, Session Hijacking, DoS-Attacken, Buffer-Overflow- bzw. Format-String-Attacken sowie jegliches weitere Ausnutzen von Schwachstellen in Betriebs- und Anwendungssystemen und Netzwerkprotokollen.

- Social-Engineering

  Bei sog. Social-Engineering-Angriffen wird versucht, Menschen mit privilegiertem Wissen insofern zu manipulieren, dass sie dem Angreifer sicherheitsrelevante Informationen, wie z. B. Passwörter, preisgeben. Beispielsweise könnte sich ein Angreifer als IT-Mitarbeiter einer Organisation ausgeben und dadurch einen arglosen Benutzer unter einem Vorwand zur Herausgabe seines Netzwerk-Passwortes bewegen. Besonders bei dieser Technik ist die Variationsmöglichkeit von Angriffsszenarios sehr hoch. Im weitesten Sinne könnte man auch Szenarien, in denen Erpressung als Mittel zur Herausgabe von sicherheitsrelevanten Informationen eingesetzt wird, als Social-Engineering bezeichnen.

- Umgehung physischer Sicherheitsmaßnahmen

  Die physische Sicherheit der technischen Infrastruktur ist eine Grundvoraussetzung zur Gewährleistung von IT-Sicherheit. Wenn physische Sicherheitsmaßnahmen überwunden werden können und auf diese Weise physischer Zugriff auf die IT-Systeme erlangt wird, ist es meist nur eine Frage der Zeit, bis auch ein Zugriff auf bzw. die Manipulation der gespeicherten Anwendungen und Daten stattfinden kann. Ein Beispiel ist das unbefugte Eindringen in das Rechenzentrum einer Organisation und das Entwenden einer Festplatte mit vertraulichen Daten. Auch das Durchsuchen von Abfällen nach Dokumenten mit sicherheitssensitiven Informationen (Dumpster Diving) gehört zu dieser Gruppe.

2.2 IT-Sicherheitsmaßnahmen

Um den beschriebenen Gefahren entgegenzuwirken, sind Maßnahmen zur Steigerung der IT-Sicherheit zu ergreifen. Dabei ist jedoch zu beachten, dass eine hundertprozentige Sicherheit grundsätzlich nicht erreicht werden kann. Es lassen sich organisatorische, wie z. B. IT Sicherheits-organisation und Eskalationsvorschriften, technische Maßnahmen, wie Zugriffsschutzmechanismen, Verschlüsselung und Firewalls zur Etablierung eines bestimmten IT-Sicherheitsniveaus unterscheiden.

Diese werden unter Berücksichtigung der unternehmensweiten IT-Sicherheitsleitlinie („IT-Security Policy“) in einem organisationsweiten IT-Sicherheitskonzept zusammengeführt.

Falls die zu prüfende Organisation kein Sicherheitskonzept bzw. keine Sicherheitsleitlinien vorlegen kann, ist es vor allem bei einer komplexen IT-Landschaft fragwürdig, ob die Durchführung eines Penetrationstests überhaupt sinnvoll ist. Vermutlich wäre es für eine Steigerung der IT-Sicherheit viel effizienter, zunächst ein geeignetes Sicherheitskonzept zu erarbeiten und umzusetzen.

2.3 Entwicklung von Penetrationstests

Der Begriff „Penetrationstest“ und die dazu durchgeführten Methoden wurden 1995 etabliert, als der erste Unix-basierte Schwachstellen-Scanner „SATAN“ [Venema95] veröffentlicht wurde. Das Programm stellte zur damaligen Zeit das erste Tool dar, das automatisiert Rechner auf Schwachstellen untersuchen konnte.

Mittlerweile existiert eine Vielzahl frei erhältlicher und kommerzieller Schwachstellen-Scanner, die meist über eine aktualisierbare Datenbank bekannter Hard- und Softwareschwachstellen verfügen. Mit Hilfe dieser Tools lassen sich auf komfortable Art und Weise Schwachstellen der zu überprüfenden Systeme identifizieren und somit Aussagen zu deren Gefährdungen treffen. Üblicherweise enthalten die hinterlegten Informationen nicht nur eine technische Beschreibung der Schwachstelle, sondern liefern zusätzlich Anweisungen, wie die identifizierte Schwachstelle durch Ändern von Konfigurationseinstellungen zu beheben ist.

Darüber hinaus gibt es im Internet eine große Zahl kostenloser Tools, mit denen Angriffe auf Internet-Computer und Netzwerke durchgeführt oder vorbereitet werden können.

2.4 Vorgehensweise für Penetrationstests

Die Vorgehensweise zur Durchführung eines Penetrationstests sollte nach dem folgendem Schema aufgebaut sein.

1. **Recherche nach Informationen über das Zielsystem**

   Im Internet erreichbare Rechner müssen über eine offizielle IP-Adresse verfügen. Frei zugängliche Datenbanken liefern Informationen über IP-Adressblöcke, die einer Organisation zugewiesen sind.

2. **Scan der Zielsysteme auf angebotene Dienste**

   Hierbei wird versucht, den oder die zu überprüfenden Rechner einem sog. Portscan zu unterziehen, wobei evtl. geöffnete Ports Rückschlüsse auf die zugeordneten Anwendungen zulassen.

3. **System- und Anwendungserkennung**

   Über das sog. „Fingerprinting“ können Namen und Version von Betriebssytemen und Anwendungen auf den Zielsystemen in Erfahrung gebracht werden.

4. **Recherche nach Schwachstellen**

   Anhand der gewonnenen Informationen können sich zielgerichtet Informationen über Schwachstellen bestimmter Betriebssyteme und Anwendungen gesucht werden.

5. **Ausnutzen der Schwachstellen**

   Gefundene Schwachstellen können dazu genutzt werden, unberechtigten Zugriff zum System zu erhalten bzw. weitere Angriffe vorzubereiten.

Die Qualität und der Nutzen eines Penetrationstests wird im Wesentlichen davon bestimmt, inwieweit dieser auf die individuelle Situation des Auftraggebers eingeht, d. h. wie viel Zeit und Ressourcen der Dienstleister auf die Ausforschung von Schwachstellen, die die konkrete IT-Infrastruktur betreffen, verwendet und wie kreativ er dabei vorgeht. Dieser Ablauf kann nicht mehr in der obigen allgemein gültigen Beschreibung dargestellt werden. Deshalb existieren große Unterschiede bezüglich der Qualität der als Penetrationstest bezeichneten Dienstleistung.

3 Einordnung und Zielsetzung von Penetrationstests

In diesem Kapitel wird beschrieben, welche Ansatzpunkte und Zugangswege für einen Penetrationstest in Betracht kommen, welche IT-Sicherheits- bzw. Schutzmaßnahmen dabei geprüft werden können und wie sich die Tests von allgemeinen IT-Sicherheitsprüfungen bzw. von IT-Revision unterscheiden.

3.1 Ansatzpunkte und Zugangswege für Penetrationstests

Typische Ansatz- bzw. Angriffspunkte für einen Penetrationstest sind Firewalls, Webserver sowie RAS Zugänge (z. B. Modems, Fernwartungszugänge) und Funknetze. Firewalls sind wegen ihrer Funktion als Übergang zwischen Internet und Firmennetz für Angriffsversuche und somit auch als

erster Ansatzpunkt für Penetrationstests prädestiniert. Das hohe Gefährdungspotential von Webservern liegt an ihren umfangreichen Funktionen und den daraus resultierenden Schwachstellen. Andere Server, die von „außen“ erreichbare Dienste wie z. B. E-Mail, FTP- und DNS anbieten, sollten ebenso wie „normale“ Arbeitsplatzrechner in den Test einbezogen werden.

3.1.1 Prüfbare IT-Sicherheitsmaßnahmen

Im Rahmen eines Penetrationstests sollten sowohl logische IT-Sicherheitsmaßnahmen wie z. B. Passwörter als auch physische Maßnahmen wie Zutrittskontrollsysteme geprüft werden. Häufig werden nur logische Sicherheitsmaßnahmen geprüft, da diese erstens größtenteils aus der Ferne über das Netzwerk getestet werden können und somit weniger Aufwand erforderlich ist und zweitens die Wahrscheinlichkeit für Angriffe auf logische IT-Sicherheitsmaßnahmen als ungleich größer angesehen wird.

3.1.2 Penetrationstest, IT-Sicherheits-Audit, IT-Revision

„Cracker“ haben das Ziel, auf geschützte Daten zuzugreifen bzw. durch böswillige Handlungen die Datenverarbeitung zu stören. Sicherheits-Audits und IT-Revisionen dienen im Gegensatz zum Penetrationstest der generellen Überprüfung der IT-Infrastruktur hinsichtlich Ordnungsmäßigkeit, Effizienz, Effektivität etc. und sind nicht zwingend auf die Aufdeckungen von angreifbaren Schwachstellen fokussiert. So wird z. B. im Rahmen eines Penetrationstests nicht geprüft, ob bestimmte Daten im Falle eines Hardwareschadens durch regelmäßige Datensicherung wiederherstellbar wären, sondern nur, ob auf diese Daten Zugriff erlangt werden könnte. Dies wird möglicherweise auch im Rahmen eines Sicherheits-Audits bzw. im Rahmen einer IT-Revision geprüft, üblicherweise aber aus einer anderen Perspektive und auch nicht in der technischen Tiefe, die einen Penetrationstest auszeichnet.

3.2 Zielsetzungen von Penetrationstests

Für eine erfolgreiche Durchführung eines Penetrationstests, die den Erwartungen des Auftraggebers entspricht, ist eine klare Zielvereinbarung unbedingt notwendig. Falls Ziele angestrebt werden, die nicht bzw. nicht effizient erreicht werden können, so sollte der Tester in der Vorbereitungsphase deutlich darauf hinweisen und alternative Vorgehensweisen wie z. B. eine IT-Revision oder IT-Sicherheitsberatung empfehlen.

Die Ziele des Auftraggebers, die mit einem Penetrationstest erreicht werden können, lassen sich in vier Gruppen einteilen:

1. Erhöhung der Sicherheit der technischen Systeme
2. Identifikation von Schwachstellen
3. Bestätigung der IT-Sicherheit durch einen externen Dritten

4. Erhöhung der Sicherheit der organisatorischen und personellen Infrastruktur

Im Ergebnis eines IT-Penetrationstests sollte daher nicht nur eine Auflistung vorhandener Schwachstellen vorhanden sein, sondern möglichst auch konkrete Lösungsvorschläge für deren Beseitigung aufgeführt werden.

Im Folgenden werden die vier Zielgruppen anhand von konkreten Beispielen erläutert.

3.2.1 Erhöhung der Sicherheit der technischen Systeme

Die meisten Penetrationstests werden mit der Zielsetzung in Auftrag gegeben, die Sicherheit der technischen Systeme zu erhöhen. Die Tests beschränken sich auf die technischen Systeme, wie Firewall, Router, Web-Server, etc., die organisatorische bzw. personelle Infrastruktur wird nicht explizit geprüft. Ein Beispiel ist ein Penetrationstest bei dem gezielt geprüft werden soll, ob es unautorisierten Dritten möglich ist, über das Internet auf Systeme innerhalb des LANs des Unternehmens zuzugreifen. Mögliche Ergebnisse bzw. Feststellungen des Tests sind nicht benötigte offene Ports der Firewall, verwundbare Versionen der eingesetzten Internet-Applikationen, Betriebssystemen.

3.2.2 Identifikation von Schwachstellen

Im Unterschied zu den anderen drei Zielen ist die Identifikation hier als Entscheidungskriterium das direkte Ziel des Tests. So kann beispielsweise vor dem Zusammenschalten zweier LANs im Rahmen eines Firmenzusammenschlusses geprüft werden, ob es möglich ist, in das neue LAN von außen einzudringen. Falls dies durch den Penetrationstest gelingt, müssen vor dem Zusammenschluss Maßnahmen zur Sicherung des Übergangs getroffen werden oder sogar vom Zusammenschluss generell Abstand genommen werden.

3.2.3 Bestätigung der IT-Sicherheit durch einen externen Dritten

Ein Penetrationstest kann auch durchgeführt werden, um eine Bestätigung eines unabhängigen, externen Dritten zu erlangen. Dabei sollte beachtet werden, dass ein Penetrationstest immer nur eine Momentaufnahme darstellt und daher keine Aussagen über das Sicherheitsniveau für die Zukunft gegeben werden kann. Dennoch kann z. B. die regelmäßige Durchführung von Penetrationstests geeignet sein, um eine erhöhte Sicherheit der Kundendaten innerhalb eines Webshops oder einer anderen Internet-Applikation zu demonstrieren.

3.2.4 Erhöhung der Sicherheit der organisatorischen/personellen Infrastruktur

Neben der technischen Infrastruktur kann ein Penetrationstest auch die organisatorische/personelle Infrastruktur, beispielsweise zur Kontrolle von Eskalationsprozeduren, prüfen. Dazu kann stufenweise der Umfang bzw. die Aggressivität des Tests gesteigert werden. Mittels Social-Engineering-Techniken, wie z. B. mit telefonischem Abfragen von Passwörtern, kann das allgemeine Sicherheitsbe-

wusstsein bzw. die Wirksamkeit von Sicherheitsleitlinien und Nutzungsvereinbarungen evaluiert werden.

Welchen Umfang solche Tests haben sollen, muss vorher sehr genau vereinbart werden (siehe auch Abschnitt 5.4 Ethische Überlegungen).

3.3 Grenzen von Penetrationstests

Da sich die Techniken der potenziellen Angreifer schnell weiterentwickeln und beinahe täglich neue Schwachstellen in aktuellen Applikationen und IT-Systemen gemeldet werden, kann aus einem einzelnen Penetrationstest keine Aussage über das Sicherheitsniveau der geprüften Systeme für die Zukunft abgeleitet werden. Im Extremfall kann unmittelbar nach Abschluss eines Penetrationstests aufgrund einer neuen Sicherheitslücke ein erfolgreicher Angriff möglich sein.

Das bedeutet jedoch keinesfalls, dass Penetrationstests an sich sinnlos sind. Die gründliche Durchführung kann zwar einen erfolgreichen Angriff nicht völlig ausschließen, sie reduziert jedoch die Wahrscheinlichkeit für einen erfolgreichen Angriff beträchtlich. Die Wirkung eines Penetrationstests ist aber aufgrund der Weiterentwicklung im IT-Bereich relativ schnell vergänglich. Je höher der Schutzbedarf der Systeme, desto häufiger sollten Penetrationstests durchgeführt werden, um die Wahrscheinlichkeit eines erfolgreichen Angriffes auf einem für das Unternehmen akzeptablen Niveau zu halten.

Ein Penetrationstest kann nicht die üblichen IT-Sicherheitsprüfungen und selbstverständlich auch keine allgemeine Sicherheitsleitlinie etc. ersetzen. So kann z. B. ein Berechtigungs- oder ein Datensicherungskonzept nur durch andere Maßnahmen effektiv und effizient geprüft werden. Ein Penetrationstest ist vielmehr eine Erweiterung der etablierten Prüfungshandlungen, die den neuen Bedrohungen begegnet.

3.4 Klassifikation

Anhand welcher Kriterien kann man einen Penetrationstest beschreiben, bzw. was unterscheidet einen Penetrationstest von einem anderen Penetrationstest? Die Unterscheidungsmerkmale wie Umfang der geprüften Systeme, die Vorsicht bzw. Aggressivität beim Testen etc., die einen bestimmten Penetrationstest charakterisieren, müssen an die Zielsetzung des Tests angepasst werden, um eine effektive und effiziente Durchführung mit kalkuliertem Risiko sicherzustellen. In Abbildung 1 ist eine Klassifikation von möglichen Penetrationstests dargestellt. Auf der linken Seite sind sechs Kriterien aufgelistet, nach denen man Penetrationstests unterscheiden kann und auf der rechten Seite sind die unterschiedlichen Werte für die Kriterien in einem kompakten Baumdiagramm zusammengefasst.

Abbildung 1: Klassifikation von Penetrationstests

Je nach Zielsetzung des Auftraggebers muss ein geeigneter Penetrationstest anhand der genannten Kriterien vereinbart werden. Dabei ist zu beachten, dass nicht alle möglichen Kombinationen sinnvolle Tests darstellen, obwohl bei der Klassifikation großer Wert auf die klare Trennung der Kriterien gelegt wurde. Ein aggressiver Test wird meistens sehr schnell erkannt und ist daher nicht optimal in Kombination mit einer verdeckten Vorgehensweise kombinierbar. Analog ist ein offensichtlicher Penetrationstest nicht geeignet, um mittels Social-Engineering-Techniken z. B. vertrauliche Informationen von den vorgewarnten Mitarbeitern zu erlangen.

Im Folgenden werden die sechs Kriterien und die möglichen Werte erläutert:

1. **Informationsbasis**: Von welchem Wissensstand über das anzugreifende Netz bzw. Objekt geht der Penetrationstester aus?

   Hier unterscheidet man grundlegend zwischen sog. Black-Box-Testing ohne jegliches Insiderwissen und dem White-Box-Testing mit Insiderwissen:

   1. Ein **Black-Box**-Test „simuliert“ realistisch einen Angriff eines typischen Internet-Hackers. Der Hacker muss die benötigten Informationen in öffentlich zugänglichen Datenbanken recherchieren oder von außen als Unternehmensfremder erfragen.

2. Bei einem **White-Box**-Test wird ein Angriff eines (Ex-) Mitarbeiters oder eines externen Dienstleisters mit bestimmten Detailkenntnissen simuliert. Der Umfang der Kenntnisse kann dabei von nur geringen Kenntnissen, wie sie z. B. ein Mitarbeiter besitzt, der nur kurze Zeit im Unternehmen beschäftigt war, bis hin zu tief gehenden Systemkenntnissen, wie sie z. B. ein externer IT-Dienstleister durch die Installation von sicherheitsrelevanten Systemen erlangt.

2. **Aggressivität**: Wie aggressiv geht der Penetrationstester beim Testen vor?

   Um eine hinreichend feine Unterscheidung zu ermöglichen, werden in dieser Studie vier Aggressivitätsstufen unterschieden:

   - Bei der niedrigsten Aggressivitätsstufe werden die Testobjekte nur **passiv** untersucht, d. h. gefundene mögliche Schwachstellen werden nicht ausgenutzt.
   - In der zweiten Aggressivitätsstufe – **vorsichtig** – werden gefundene Schwachstellen nur dann ausgenutzt, wenn nach bestem Wissen eine Beeinträchtigung des untersuchten Systems ausgeschlossen werden kann, z. B. die Benutzung von bekannten Default-Passwörtern oder das Ausprobieren von Verzeichniszugriffen bei einem Web-Server.
   - In der nächste Stufe – **abwägend** – wird auch versucht, Schwachstellen auszunutzen die unter Umständen zu Systembeeinträchtigungen führen könnten. Darunter fallen z. B. das automatische Durchprobieren von Passwörtern und das Ausnutzen von bekannten Buffer-Overflows bei genau identifizierten Zielsystemen. Allerdings wird vorher abgewägt, wie wahrscheinlich ein Erfolg ist und wie stark die Konsequenzen wären.
   - In der höchsten Aggressivitätsstufe – **aggressiv** – wird versucht, alle potentiellen Schwachstellen auszunutzen, z. B. werden Buffer-Overflows auch bei nicht eindeutig identifizierten Zielsystemen eingesetzt oder Sicherungssysteme werden durch gezielte Überlastung (Denial of Service, DoS-Attacken) deaktiviert. Dem Auftragnehmer muss bewusst sein, dass neben den zu testenden Systemen auch benachbarte Systeme oder Netzkomponenten bei diesen Tests ausfallen können.

3. **Umfang**: Welche Systeme sollen getestet werden?

   Bei einem erstmaligen Penetrationstest ist grundsätzlich eine vollständige Überprüfung empfehlenswert, damit keine Sicherheitslücken auf den nicht-geprüften Systemen übersehen werden.

   Der Aufwand für einen Penetrationstest hängt üblicherweise direkt vom Umfang der zu untersuchenden Systeme ab. Zwar können identische und nahezu identische Systeme teilweise

automatisch in einem Arbeitsschritt untersucht werden, sobald aber eine abweichende Konfiguration gefunden wird, muss jedes System individuell behandelt werden:

- Ist vereinbart, dass nur ein bestimmtes Teilnetz, System oder ein bestimmter Dienst geprüft werden soll, so wird der Penetrationstest in dieser Studie als **fokussiert** bezeichnet. Dieser Umfang bietet sich z. B. nach einer Änderung oder Erweiterung der Systemlandschaft an. Der Test kann dann aber naturgemäß auch nur Aussagen über das getestete System und keine allgemeinen Hinweise zur IT-Sicherheit liefern.
- Bei einem **begrenzten** Penetrationstest wird eine begrenzte Anzahl von Systemen oder Diensten untersucht. So können beispielsweise alle Systeme in der DMZ geprüft werden oder auch Systeme, die einen funktionalen Verbund bilden.
- Der **vollständige** Test prüft alle erreichbaren Systeme. Dabei ist zu beachten, dass auch bei einem vollständigen Test u. U. bestimmte Systeme, z. B. ausgelagerte und extern gehostete dennoch nicht geprüft werden dürfen (siehe 5.1).

4. **Vorgehensweise**: Wie „sichtbar“ geht das Team beim Testen vor?

   Sollen neben den primären Sicherheitssystemen auch sekundäre wie beispielsweise ein IDS oder organisatorische und personelle Strukturen wie Eskalationsprozeduren geprüft werden, so muss die Vorgehensweise bei der Durchführung des Penetrationstests entsprechend angepasst werden:

   - Zur Prüfung von sekundären Sicherheits-Systemen und der vorhandenen Eskalationsprozeduren sollten – zumindest am Anfang – **verdeckte** Penetrationstests durchgeführt werden, d. h., dass in der Erkundungsphase nur solche Methoden zum Einsatz kommen, die nicht direkt als Angriffsversuche erkannt werden können.
   - Falls die verdeckte Vorgehensweise keine Reaktionen ausgelöst hat oder ein White-Box-Test mit Einbeziehung der Systemverantwortlichen durchgeführt wird, so können auch **offensichtliche** Methoden wie z. B. umfangreiche Port-Scans mit direktem Connect angewendet werden. Bei einem offensichtlichen White-Box-Test können auch Mitarbeiter des Auftraggebers mit in das Team integriert werden, was besonders bei hochkritischen Systemen aufgrund der schnelleren Reaktionsmöglichkeiten auf unvorhergesehene Probleme ratsam ist.

5. **Technik**: Welche Techniken werden beim Testen eingesetzt?

   Beim klassischen Penetrationstest werden die Systeme nur über das Netzwerk angegriffen. Ergänzend können die Systeme auch mittels sonstigen physischen Angriffen und Social-Engineering-Techniken attackiert werden:

- Der Penetrationstest über das **Netzwerk** entspricht dem normalen Vorgehen und simuliert einen typischen Hackerangriff. Die meisten IT-Netzwerke verwenden z. Zt. das TCP/IP Protokoll, so dass man auch von IP-basierten Penetrationstests spricht.
- Neben TCP/IP Netzwerken existieren **weitere Kommunikationsnetze**, die ebenfalls für Angriffe genutzt werden können. Dazu zählen neben Telefon- bzw. Fax-Netzen auch drahtlose Netze für mobile Kommunikation, z. B. auf Basis von IEEE 802.11(b) und zukünftig wohl auch BlueTooth Verbindungen.
- Mittlerweile sind Sicherheitssysteme wie Firewalls etc. weitverbreitet und die Konfigurationen dieser Systeme meist auf einem hohen Sicherheitsniveau, sodass ein Angriff unter Überwindung dieser Systeme nicht mehr oder nur mit sehr hohem Aufwand möglich ist. Oftmals ist es dann einfacher und schneller, die „gewünschten“ bzw. „gesuchten“ Daten durch Umgehung dieser Systeme durch einen direkten **physischen Zugriff** zu erlangen. Hierzu zählt z. B. der direkte Datenzugriff an einer nicht-passwortgeschützten Arbeitsstation nach Erlangung von unberechtigtem Zugang in die Gebäude und/oder Serverräume.
- Das schwächste Glied in der Kette der Sicherungssysteme ist oftmals der Mensch. Daher sind **Social-Engineering**-Techniken, die unzureichende Sicherheitskenntnisse oder ein mangelndes Sicherheitsbewusstsein ausnutzen, häufig erfolgreich. Diese Tests bieten sich beispielsweise nach Einführung einer allgemeinen Sicherheitsleitlinie an, um den Grad der Umsetzung bzw. die Akzeptanz zu evaluieren. Falsche Annahmen über die vermeintliche Wirksamkeit der Richtlinien führen häufig zu Sicherheitsrisiken, die bei korrekter Einschätzung durch zusätzliche Maßnahmen abgefangen werden könnten. Wie weit diese Tests gehen dürfen, wird in den Abschnitten „5.4“: Ethische Überlegungen und „4.2“: Bei der Durchführung von Penetrationstests zu beachtende gesetzliche Rahmenbedingungen ausführlich behandelt.

6. **Ausgangspunkt**: Von wo aus wird der Penetrationstest durchgeführt?

   Der Ausgangspunkt des Penetrationstests, d. h. der Punkt, an dem der Penetrationstester seinen Rechner ans Netz anschließt bzw. von dem seine Angriffsversuche ausgehen, kann außerhalb oder innerhalb des Netzwerkes oder der Gebäude des Auftraggebers liegen:

   - Die meisten Hackerangriffe erfolgen über die Netzwerkanbindung an das Internet. Daher kann ein Penetrationstest **von außen** die potenziellen Risiken eines solchen Angriffs erfassen und bewerten. Typischerweise werden hierbei die Firewall und Systeme in der DMZ sowie RAS-Verbindungen untersucht.

- Bei einem Penetrationstest **von innen** müssen üblicherweise keine Firewalls bzw. Eingangskontrollen überwunden werden, um Zugang zu den internen Netzen zu erhalten. Daher kann mit einem Test von innen bewertet werden, was z. B. bei einem Fehler in der Firewall-Konfiguration oder bei einem erfolgreichen Angriff auf die Firewall passieren könnte bzw. welche Zugriffsmöglichkeiten Personen mit Zugang zum internen Netzwerk erlangen könnten.

3.5 Mehrstufiges Vorgehen

Oftmals ist eine Kombination von verschiedenen Penetrationstests nach der dargestellten Klassifizierung zur weiteren Risikominimierung empfehlenswert. So kann beispielsweise zuerst ein vorsichtiger, verdeckter Black-Box-Test von außen und dann im zweiten Schritt ein aggressiver, offensichtlicher White-Box-Test von innen durchgeführt werden. So kombiniert man die Vorteile eines Black-Box-Tests, die möglichst realistische Simulation eines echten Angriffs, mit den Vorteilen eines White-Box-Tests hinsichtlich Effizienz und Schadensminimierung.

4 Rechtliche Überlegungen

Die rechtlichen Überlegungen, die bezüglich Penetrationstests vorgenommen werden müssen, können im Wesentlichen in drei Abschnitte unterteilt werden:

- Rechtliche Überlegungen, die ein Unternehmen oder eine Behörde zur Durchführung eines Penetrationstests veranlassen bzw. motivieren können.
- Rechtliche Vorschriften und Grundsätze, die der Auftragnehmer während der Durchführung eines Penetrationstests beachten sollte und die im Vorfeld des Tests mit dem Auftraggeber geklärt werden sollten.
- Rechtliche Gesichtspunkte, die der Vertragsgestaltung zwischen Auftraggeber und Penetrationstester zugrunde liegen.

4.1 Gesetzliche Vorschriften als Motivation für Penetrationstests

Zwar existieren keine Gesetze, die eine Firma oder Behörde unmittelbar dazu verpflichten, Penetrationstests durchführen zu lassen, doch existieren verbindliche Vorschriften bezüglich

- der Handhabung der Sicherheit und der Verfügbarkeit von steuerrechtlich und handelsrechtlich relevanten Daten,
- des Umgangs mit personenbezogenen Daten,
- der Einrichtung und Ausgestaltung eines internen Kontrollsystems.

Um unternehmensrelevante Daten zu schützen, ergreifen Unternehmen regelmäßig Maßnahmen, die die Verfügbarkeit, Vertraulichkeit und Integrität der Daten gewährleisten sollen bzw. die den Zugriff nur für autorisierte Personen sicherstellen sollen. Zu diesen Maßnahmen zählen beispielsweise Sicherheitskonzepte, Berechtigungskonzepte oder Firewallsysteme. Allein durch die Etablierung derartiger Sicherheitssysteme ist eine Erfüllung der gesetzlichen Vorgaben jedoch nicht gewährleistet. Vielmehr muss jeweils geprüft werden, ob die Systeme den gesetzlichen Vorgaben und Anforderungen genügen. Penetrationstests sind dabei u. a. ein geeignetes Mittel, die Wirksamkeit solcher Maßnahmen in Teilbereichen zu verifizieren.

Die wichtigsten gesetzlichen Vorschriften, die bei der Einrichtung und Unterhaltung von Sicherheits- und Berechtigungssystemen zu beachten sind, werden nachfolgend im Kontext zur Zweckmäßigkeit des Einsatzes von Penetrationstests dargestellt.

4.1.1 Handelsgesetzbuch (HGB)

Das Handelsgesetzbuch (HGB) schreibt dem „Kaufmann“ in § 238 Abs. 1 vor, Bücher nach den Grundsätzen ordnungsmäßiger Buchführung (GoB) bzw. nach den Grundsätzen ordnungsmäßiger DV-

gestützter Buchführungssysteme (GoBS) (BMF Schreiben an die obersten Finanzbehörden der Länder vom 7 November 1995) zu führen.

Vorschriften zu dem Internen Kontrollsystem (IKS) eines Unternehmens finden sich im 4. Abschnitt der GoBS:

- Rd-Nr. 4.1: „Als IKS wird grundsätzlich die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen bezeichnet, die die folgenden Aufgaben haben: Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art. [...]“

Bestimmungen zur Datensicherheit finden sich unter Abschnitt 5 der GoBS:

- Rd-Nr. 5.1: „Die starke Abhängigkeit der Unternehmung von ihren gespeicherten Informationen macht ein ausgeprägtes Datensicherheitskonzept für das Erfüllen der GoBS unabdingbar. [...]“
- Rd-Nr. 5.3: „Diese Informationen sind gegen Verlust und gegen unberechtigte Veränderung zu schützen. [...]“
- Rd-Nr. 5.5.1: „Der Schutz der Informationen gegen unberechtigte Veränderungen ist durch wirksame Zugriffs- bzw. Zugangskontrollen zu gewährleisten. [...]“

Den vorgenannten Bestimmungen ist zu entnehmen, dass hohe Anforderungen an die Datensicherheit in Unternehmen gestellt werden. Diese gesetzlichen Vorgaben können nur durch ein IT-Sicherheitskonzept (in der Terminologie der GoBS als „Datensicherheitskonzept“ bezeichnet) im Rahmen des Internen Kontrollsystems realisiert werden. Ob ein solches Sicherheitskonzept den hohen gesetzlichen Anforderungen genügt, kann u a. mit Hilfe von Penetrationstests stichprobenartig überprüft werden.

4.1.2 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Seit Inkrafttreten des KontraG im Mai 1998 sind Vorstände von Aktiengesellschaften verpflichtet, ein Risikomanagementsystem zu etablieren und erweiterte Berichtspflichten gegenüber dem Aufsichtsrat zu erfüllen. § 91 Abs. 2 Aktiengesetz (AktG) wurde wie folgt neu gefasst:

- § 91 Abs 2 AktG: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. [...]“

Die geänderten Regelungen gelten über die so genannte „Ausstrahlungswirkung“ auch für die Geschäftsführung einer GmbH.

Wie ein Risikomanagementsystem konkret auszugestalten ist, hat der Gesetzgeber nicht ausdrücklich bestimmt. Der Gesetzesbegründung ist jedoch zu entnehmen, dass Risikomanagementsysteme Elemente wie ein Frühwarnsystem, ein internes Überwachungssystem einschließlich einer Revision

und ein Controlling enthalten müssen. [Andersen99, S.20]. In diesem Zusammenhang sind Penetrationstests eine geeignete Maßnahme zur Prüfung des IT-bezogenen Teils des Frühwarnsystems oder von Bestandteilen der Revision.

4.1.3 Kreditwesengesetz (KWG)

Banken und weitere Organisationen der Finanzdienstleistungsbranche unterliegen den Bestimmungen des Kreditwesengesetzes (KWG). Eine Besonderheit des KWG ist, dass die Bundesanstalt für Finanzdienstleistungsaufsicht berechtigt ist, bei allen Finanzdienstleistungsunternehmen Prüfungen durchzuführen, die sich über alle geschäftlichen Bereiche des Unternehmens erstrecken können.

§ 44 Abs. 1 KWG enthält folgende Regelung:

- „[...] Die Bundesanstalt kann, auch ohne besonderen Anlass, bei den Instituten Prüfungen vornehmen und die Durchführung der Prüfungen der Deutschen Bundesbank übertragen. [...].“

Insbesondere bei Banken, die Finanzdienstleistungen über das Internet zur Verfügung stellen, kann der Themenbereich Internet-Sicherheit zum Gegenstand einer Prüfung nach § 44 Abs. 1 KWG werden.

Für diese bietet es sich daher an, Penetrationstests im Vorfeld einer solchen Prüfung einzusetzen, um die Sicherheit der eingesetzten Internet-Anwendungen zu testenbzw. um Schwachstellen zu identifizieren und Handlungsempfehlungen bei eventuellen Defiziten auszusprechen.

4.1.4 Verordnungen und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin)

Die Bundesanstalt für Finanzdienstleistungsaufsicht (früher: Bundesaufsichtsamt für das Kreditwesen - BAFin) erlässt auf der Basis gesetzlicher Ermächtigungen u. a. Verordnungen und veröffentlicht Verlautbarungen, die Banken und andere Finanzdienstleister betreffen, über die die BAFin die Aufsicht führt. In Bezug auf Penetrationstests ist besonders folgende Verlautbarung interessant:

„Verlautbarung über Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstituten“. In dieser Verlautbarung werden u. a. die Anforderungen an das Risikomanagementsystem und die Ausgestaltung der Internen Revision definiert.

Zum Risikomanagementsystem werden in dieser Verordnung u.a. folgende Aussagen gemacht:

- Rd-Nr. 3.1 Anforderungen an das System: „[...] [Das Risikomanagementsystem] soll in ein möglichst alle Geschäftsbereiche der Bank umfassendes Konzept zur Risikoüberwachung und -steuerung eingegliedert sein und dabei die Erfassung und Analyse von vergleichbaren Risiken aus Nichthandelsaktivitäten ermöglichen. [...]“

- Rd.-Nr. 3.4 Betriebsrisiken: „[...] Eine schriftliche Notfallplanung hat u.a. sicherzustellen, dass beim Ausfall der für das Handelsgeschäft erforderlichen technischen Einrichtungen kurzfristig einsetzbare Ersatzlösungen zur Verfügung stehen. Darüber hinaus ist auch Vorsorge für mögliche Fehler in der angewandten Software und unvorhergesehene Personalausfälle zu treffen. Die Verfahren, Dokumentationsanforderungen, DV-Systeme und Notfallpläne, die im Handelsgeschäft angewandt werden, sind regelmäßig zu überprüfen.“

Durch den Einsatz von Penetrationstests können potenzielle Auswirkungen eines Angriffes besser abgeschätzt werden. So kann eine konkrete Aussage zur Funktionsfähigkeit des Risikomanagementsystems getroffen werden.

Bezüglich der Ausgestaltung der Internen Revision enthält die Verlautbarung folgende Anforderungen:

- Rd.-Nr. 5 Revisionen: „Die Einhaltung der Mindestanforderungen ist von der Innenrevision in unregelmäßigen, angemessenen Abständen zu prüfen. Hierbei sind im Sinne einer risikoorientierten Prüfung die wesentlichen Prüfungsfelder mindestens jährlich zu prüfen. Jeder Teilbereich der Mindestanforderungen ist zumindest in einem Turnus von drei Jahren zu prüfen, der Prüfungsturnus ist in einem Prüfplan zu dokumentieren.

  Als wesentliche Prüfungsfelder sind anzusehen:

  - Veränderungen bei den EDV-Systemen.

Mit Hilfe von Penetrationstests kann eine risikoorientierte Überprüfung der wesentlichen Prüfungsfelder innerhalb einer IT-Revision wirksam unterstützt werden.

4.1.5 Bundesdatenschutzgesetz (BDSG)

Datenschutzrechtliche Vorschriften finden sich im Landes- wie im Bundesrecht; sie regeln den Umgang von öffentlichen und nicht-öffentlichen Stellen mit personenbezogenen Daten.

Das Bundesdatenschutzgesetz (BDSG) gilt gem. § 1 II BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist [...],
3. nicht öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben [...].

- § 9 S. 1 BDSG Technische und organisatorische Maßnahmen: „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.“

Die auf die im Gesetzestext verwiesene Anlage enthält Anforderungen bezüglich Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle.

- § 9a BDSG Datenschutzaudit: „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. [...]“

Penetrationstests können als Instrument einer effizienten Prüfung innerhalb eines Datenschutzaudits eingesetzt werden, um Aussagen zur Umsetzung der Vorschriften und der Wirksamkeit des Datenschutzkonzeptes zu gewinnen.

Hinweis: EU-Datenschutzrichtlinie (95/46/EG)

Mit der Novellierung des BDSG vom 18. Mai 2001 wurde die EU-Datenschutzrichtlinie 95/46/EG in Deutschland umgesetzt.

Art. 17 Abs. 1 der Richtlinie weist auf die Notwendigkeit eines Sicherheitskonzepts von Unternehmen in der EU hin: „Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten über ein Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind. [...]“

Eine weitergehende Novellierung des BDSG ist mit Umsetzung der Europäischen Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) zu erwarten, die zu Anpassungen in den Bereichen Verarbeitung personenbezogener Daten und Schutz der Privatsphäre im Bereich der Telekommunikation an die neuere Entwicklung der Märkte und Technologien für elektronische Kommunikationsdienste führen wird.

- Artikel 4 Abs. 1 [Betriebssicherheit]: „Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die

Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. [...]

In der Richtlinie ist eine Frist zur Umsetzung bis spätestens 31.10.2003 vorgesehen.

4.1.6 Staatsvertrag für Mediendienste (MDStV)

Der Staatsvertrag für Mediendienste hat das Ziel, einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten von Informations- und Kommunikationsdiensten, die an die Allgemeinheit gerichtet sind, zu schaffen.

Der MDStV richtet sich hauptsächlich an Unternehmen, die gewerbsmäßig Mediendienste anbieten. Dabei wird zwischen „Verteildiensten“ und „Diensteanbietern“ unterschieden. Ein Verteildienst bezeichnet den Anbieter eines Mediendienstes (z. B. Teleshopping). Ein Diensteanbieter ermöglicht den Zugang zur Nutzung eines Mediendienstes. Stellt ein Unternehmen oder eine Behörde seinen Mitarbeitern einen Internetzugang zur Nutzung bereit, so wird auch dieses Unternehmen zum Diensteanbieter und hat entsprechend die Vorschriften des MDStV zu beachten.

Folgende Paragrafen lassen unter Prüfungsgesichtspunkten einen Bezug zu Penetrationstests herstellen:

- § 13 Abs. 2 MDStV [Pflichten des Anbieters]: „Der Anbieter von Mediendiensten hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass [...] 3. der Nutzer Mediendienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.“[...].
- § 17 MDStV [Datenschutz-Audit]: „Zur Verbesserung von Datenschutz und Datensicherheit können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. [...]“

Penetrationstests lassen sich zur Prüfung der festgelegten technischen und organisatorischen Vorkehrungen sowie des Datenschutzkonzeptes konkret einsetzen.

4.1.7 Teledienstegesetz (TDG) und Teledienstedatenschutzgesetz (TDDSG)

Das Teledienstegesetz richtet sich an Diensteanbieter, die „eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln“. Ein Teledienst ist dabei beispielsweise ein Angebot im Bereich der Individualkommunikation oder eine interaktive Bestellmöglichkeit. In diesem Sinne ist beispielsweise jede Organisation, die Informationen auf einer Internet-Webseite veröffentlicht oder die Möglichkeit zur Kontaktaufnahme über E-Mail bietet, ein Diensteanbieter.

Das Teledienstedatenschutzgesetz gibt den datenschutzrechtlichen Rahmen vor, in dem Diensteanbieter die personenbezogenen Daten der Nutzer erheben, verarbeiten und nutzen dürfen.

- § 4 Abs. 4 TDDSG [Pflichten des Diensteanbieters]: „Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass, [...] der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.“

Hierbei können Penetrationstests wiederum als Kontrollinstrumente zur Überprüfung der Wirksamkeit des Datenschutzkonzeptes eingesetzt werden.

4.1.8 Telekommunikationsgesetz (TKG)

Dieses Gesetz richtet sich an geschäftsmäßige Erbringer von Telekommunikationsdiensten. Davon sind in erster Linie Telefongesellschaften und Internetdienstleister betroffen. Auch Unternehmen, deren Mitarbeiter ihren Telefonanschluss oder ihren Internetzugang am Arbeitsplatz auch zu privaten Zwecken nutzen, zählen als Erbringer von Telekommunikationsdiensten und fallen somit in den Anwendungsbereich. [LfDN99]

Ziel des Telekommunikationsgesetzes (TKG) ist unter anderem die Wahrung des Fernmeldegeheimnisses im Bereich der Telekommunikation.

- § 85 Abs. 2 TKG [Fernmeldegeheimnis] : „Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. [...]
- § 87 Abs. 1 TKG [Technische Schutzmaßnahmen] : „Wer Telekommunikationsanlagen betreibt, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, hat bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze [...]

  2. der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe, [...]

  4. von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen

  zu treffen.

Penetrationstests bieten auch hier eine Möglichkeit zur Überprüfung des IT-Sicherheitskonzeptes.

4.1.9 Strafrechtliche Vorschriften

In den letzten Jahren hat die Computerkriminalität in erheblichem Maße zugenommen. Insgesamt sind die strafrechtlichen Sanktionsmöglichkeiten allerdings eher beschränkt, so dass das Ziel, einen Rückgang der Computerdelikte durch die Schaffung neuer Straftatbestände zu erreichen, bisher nicht verwirklicht werden konnte. Die im deutschen Strafrecht bisher sehr lückenhaft geregelten Tatbestände

bieten unter generalpräventiven Gesichtspunkten keinen wirksamen Schutz. Hinzu kommen regelmäßig Beweisschwierigkeiten.

Die im Zusammenhang mit Computerkriminalität relevanten Vorschriften des Strafgesetzbuchs (StGB) finden sich hauptsächlich in den Abschnitten „Verletzung des persönlichen Lebens- und Geheimbereichs“, „Betrug und Untreue“, „Urkundenfälschung“ und „Sachbeschädigung“.

Im Folgenden wird ein kurzer Überblick über die Straftatbestände gegeben, die durch unbefugte Eingriffe in Datenverarbeitungsanlagen verwirklicht sein können.

- § 202a Abs. 1 (1) StGB [Ausspähen von Daten]: „Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“

Dieser Straftatbestand schützt primär alle gespeicherten und im Übermittlungsstadium befindlichen Daten vor unbefugtem Zugriff; Tathandlung ist das Verschaffen von Daten.

§ 263a StGB [Computerbetrug]: „Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Die Manipulation eines Datenverarbeitungsvorgangs mit der Absicht, sich oder einem anderen einen rechtswidrigen Vermögensvorteil zu verschaffen, ist strafbar. Der Straftatbestand des § 263a StGB setzt weiter subjektiv voraus, dass der Täter vorsätzlich handelt und in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen.

- § 268 Abs. 1 StGB [Fälschung technischer Aufzeichnungen]: „Wer zur Täuschung im Rechtsverkehr 1.) eine unechte technische Aufzeichnung herstellt oder eine technische Aufzeichnung verfälscht oder 2.) eine unechte oder verfälschte technische Aufzeichnung gebraucht wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Technische Aufzeichnung bezeichnet gem. § 268 Abs. 2 StGB „eine Darstellung von Daten, Mess- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbsttätig bewirkt wird, den Gegenstand der Aufzeichnung allgemein oder für Eingeweihte erkennen lässt und zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist“. Tathandlung des § 268 Abs. 1 StGB ist sowohl das Herstellen einer unechten technischen Aufzeichnung, das Verfälschen einer technischen Aufzeichnung als auch das Gebrauchen einer unechten oder verfälschten technischen Aufzeichnung. Allerdings muss der Täter, um den Tatbestand des § 268 I StGB weiter zu

erfüllen, zur Täuschung im Rechtsverkehr handeln bzw. gem. § 270 StGB die Datenverarbeitung fälschlich beeinflussen.

- § 269 Abs. 1 StGB [Fälschung beweiserheblicher Daten]: „Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“

Das zu § 268 I StGB gesagte, findet auch in diesem Fall entsprechende Anwendung.

- § 303a Abs. 1 StGB [Datenveränderung]: Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten ist durch diesen Paragrafen unter Strafe gestellt.

- § 303b StGB [Computersabotage]: „Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch dass er 1.) eine Tat nach § 303a begeht oder 2.) eine Datenverarbeitungsanlage oder einen Datenträger zerstört, unbrauchbar macht beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“

4.1.10 Europäische Cybercrime-Konvention

Die Europäische Cybercrime-Konvention wurde am 8. November 2001 durch das Ministerkomitee des Europarates verabschiedet mit dem Ziel, Gesetze und Vorgehensweisen zur Bekämpfung von Computerkriminalität bereitzustellen. Sie wurde von Deutschland und weiteren Mitgliedsstaaten des Europarates unterzeichnet, eine Ratifizierung erfolgt jedoch noch nicht.

In Kapitel 2 der Cybercrime-Konvention [Measures to be taken at the national level] werden Sachverhalte beschrieben, die ein Land in Bezug auf die Bekämpfung der Computerkriminalität zwingend unter Strafe zu stellen hat.

Die bezüglich Penetrationstests relevanten Inhalte der Konvention finden sich vor allem in den Titeln 1 und 2 der Sektion 1 [Substantive criminal law].

- Titel 1: [Offences against the confidentiality, integrity and availability of computer data and systems] Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen
    - Artikel 2: [Illegal access] Unberechtigter Zugriff / Unbefugtes Eindringen in Computersysteme und Netzwerke

  - Artikel 3: [Illegal interception] Unbefugtes Abhören von Netzwerkverkehr
  - Artikel 4 [Data interference] Unberechtigtes Ändern von Daten
  - Artikel 5 [System interference] Beeinträchtigung oder Sabotage von Computersystemen
  - Artikel 6 [Misuse of devices] Besitz und Missbrauch von Systemen und Tools, die geeignet sind, eine Handlung wie in Artikel 2-5 durchzuführen. Allerdings bezieht sich dieser Artikel nicht auf den autorisierten Gebrauch von Sicherheitstools, die zu Schutzzwecken wie Penetrationstests eingesetzt werden.
- Titel 2 [Computer-related offences] Computerbezogene Straftaten
  - Artikel 7 [Computer related forgery] Fälschungen mit Hilfe eines Computers
  - Artikel 8 [Computer related fraud] Computerbetrug

Insbesondere in Art. 6 der Konvention wird explizit klargestellt, dass ein autorisierter Einsatz von „Hacker- und Sicherheitstools“ nicht dem Zweck des Artikels widerspricht . Auch ist in der vorliegenden Cybercrime-Konvention nicht beabsichtigt, die Arbeit eines Penetrationstesters zu behindern, indem er einer möglichen Strafbarkeit durch seine Tätigkeit gegenüberstände. Es bleibt allerdings insoweit noch einer entsprechenden Umsetzung ins deutsche Recht abzuwarten.

4.2 Bei der Durchführung von Penetrationstests zu beachtende gesetzliche Rahmenbedingungen

Im Zuge eines Penetrationstests werden durch den Tester unter anderem Handlungen ausgeführt die, wenn sie nicht mit der Einwilligung des Auftraggebers geschehen, gegen geltende Gesetze verstoßen können.

4.2.1 Strafrechtliche Vorschriften

Wenngleich der Penetrationstester zumeist schon nicht tatbestandsmäßig handeln wird, da ihm besondere Absichten – wie z. B. die rechtswidrige Bereicherungsabsicht – fehlen. Außerdem sind diese Eingriffe, deren Inhalt und Umfang mit dem Auftraggeber abgestimmt sind, durch Einwilligung gerechtfertigt.

Wesentlich ist daher die exakte Festlegung des beauftragten Handlungsrahmens zwischen dem Auftraggeber und dem Auftragnehmer (vgl. dazu auch Gliederungspunkt 4.3.3 „Vertragsgegenstand“). Es ist zweckmäßig, die erforderliche Einwilligung nach Festlegung des konkreten Handlungsrahmens vor

Beginn der Durchführung des Penetrationstests in Form einer gesonderten Erklärung des Auftraggebers einzuholen.

Darüber hinaus sind folgende Vorschriften im Hinblick auf die Einwilligung des Auftraggebers von Bedeutung:

Zugangskontrolldiensteschutzgesetz (ZKDSG)

Das ZKDSG regelt den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten. Dabei wird unter einem zugangskontrollierten Dienst u.a. ein Teledienst im Sinne von § 2 des TDG oder ein Mediendienst im Sinne von § 2 des MDStV verstanden. Ein Zugangskontrolldienst ist ein technisches Verfahren oder eine Vorrichtung, die die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglicht.

Mit der Verabschiedung dieses Gesetzes wollte der Gesetzgeber den Schutz von kostenpflichtigen Diensten wie beispielsweise Pay-TV vor unbefugtem Umgehen der Sicherheitsmechanismen gewährleisten.

- § 3 ZKDSG [Verbot von gewerbsmäßigen Eingriffen zur Umgehung von Zugangskontrolldiensten]: „Verboten sind 1.) die Herstellung, die Einfuhr und die Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, 2.) der Besitz, die technische Einrichtung, die Wartung und der Austausch von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, 3.) die Absatzförderung von Umgehungseinrichtungen.

Ein passwortgeschützter WWW- oder FTP-Server stellt beispielsweise einen zugangskontrollierten Dienst dar. Es ist Sinn eines Penetrationstests, einen vorhandenen Schutzmechanismus zu umgehen. Deshalb ist, sobald der Penetrationstest mit Hilfe von Tools (Umgehungsvorrichtungen) durchgeführt wird, der Verstoß gegen das ZKDSG bei einem Penetrationstest nicht vermeidbar. Auch wird ein Penetrationstester regelmäßig die Voraussetzung erfüllen, Hacker- und Sicherheitstools zu gewerblichen Zwecken einzusetzen. Demnach könnte sich ein Penetrationstester, der einen Exploit zum Remote-Zugriff auf einem passwortgeschützten Webserver besitzt, ordnungswidrig verhalten und mit einer Geldbuße bis zu 50.000 € konfrontiert werden. [Emmert02, S.6]. Sinnvoll erscheint es auch in diesen Fällen zu sein, die entsprechende Erlaubnis des Berechtigten für eventuelle tatbestandsmäßige Handlungen einzuholen.

Telekommunikationsgesetz (TKG)

Folgende Bestimmungen des TKG können im Rahmen des TKG für einen Penetrationstester relevant sein:

- § 65 TKG Abs. 1 [Missbrauch von Sendeanlagen]: „Es ist verboten, Sendeanlagen zu besitzen [...], die ihrer Form nach einen anderen Gegenstand vortäuschen [...] und auf-

grund dieses Umstandes dazu geeignet sind, das nichtöffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören.“

- § 86 TKG [Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen]: „Mit einer Funkanlage dürfen Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden. [...]“

Mit diesen Vorschriften werden Handlungen, die bei Penetrationstests durchgeführt werden, wie beispielsweise der Einsatz von Netzwerk-Sniffern zum Abhören des Netzwerk-Verkehrs, untersagt, soweit diese nicht von den Berechtigten zuvor erlaubt wurden.

Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme

Die Europäische Kommission hat am 19.04.2002 den Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme vorgelegt. Mit dem Rahmenbeschluss sollen die strafrechtlichen Vorschriften für Angriffe auf Informationssysteme unter den Mitgliedstaaten angeglichen und die Zusammenarbeit zwischen den Behörden verbessert werden.

Das gesamte Werk umfasst 14 Artikel, von denen in Artikel 3 und 4 Straftaten näher beschrieben werden:

- Artikel 3 [Rechtswidriger Zugang zu Informationssystemen]: Die Mitgliedsstaaten stellen sicher, dass der vorsätzliche und unrechtmäßige Zugang zu einem Informationssystem unter Strafe gestellt wird, sofern diese Handlung 1.) gegen einen Teil eines spezifischen Schutzmaßnahmen unterliegenden Informationssystems gerichtet ist oder 2.) mit der Absicht begangen wird, einer natürlichen oder juristischen Person Schaden zuzufügen, oder 3.) mit der Absicht begangen wird, einen wirtschaftlichen Vorteil zu bewirken.
- Artikel 4 [Rechtswidriger Eingriff in Informationssysteme]: Die Mitgliedstaaten stellen sicher, dass die nachstehenden vorsätzlichen und unrechtmäßigen Handlungen unter Strafe gestellt werden: a) schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingabe, Übermittlung, Beschädigung, Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten; b) Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten eines Informationssystems, sofern dies in der Absicht geschieht, einer natürlichen oder einer juristischen Person Schaden zuzufügen.

Die weitere Entwicklung des Rahmenbeschlusses bleibt abzuwarten. Allerdings wird man heute schon sagen können, dass ein Penetrationstester, der mit Einverständnis seines Auftraggebers handelt und sich in dessen festgelegten Handlungsrahmen hält, auch bei Durchsetzung dieses Rahmenbeschlusses von einer Strafbarkeit nicht erfasst wird, da ihm in den meisten Fällen bereits der Vorsatz zu einer

strafbaren Handlung fehlen würde oder sein Handeln infolge einer Einwilligung des Berechtigten gerechtfertigt wäre.

4.2.2 Betriebsverfassungsgesetz (BetrVG)

Existiert in dem Unternehmen, das den Penetrationstest in Auftrag gibt ein Betriebsrat, so ist darauf zu achten, dass dem Betriebsrat jedenfalls ein Informationsrecht zusteht (§ 80 II BetrVG). Im Hinblick auf die Regelung in § 87 Abs. 1 Nr. 6 BetrVG sollte der Betriebsrat in die Planung der Durchführung von Penetrationstests einbezogen werden.

- § 87 Abs. 1 Nr. 6 BetrVG [Mitbestimmungsrechte]: „Der Betriebsrat hat [...], in folgenden Angelegenheiten mitzubestimmen:
    - bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Der Zweck eines Penetrationstests besteht darin, vorhandene Sicherheitsvorkehrungen auf ihre Wirksamkeit hin zu überprüfen. Mitunter kann ein Penetrationstest Instrument zur Beurteilung von Leistungen der Mitarbeiter darstellen. Beispielsweise wird beim Einsatz von Social-Engineering-Techniken das Verhalten von Mitarbeitern explizit untersucht.

Auch wenn die Überwachung oder die Leistungsbeurteilung der Mitarbeiter nicht der Hauptzweck eines Penetrationstests darstellen wird, sind die Ergebnisse eines Penetrationstests grundsätzlich hierzu geeignet. Nach BAG ist allein entscheidend, ob die Einrichtung zur Überwachung objektiv dazu geeignet ist, ohne Rücksicht darauf, ob der Arbeitgeber dieses Ziel verfolgt und die durch die Überwachung gewonnenen Daten auch auswertet. Eine frühzeitige Einbeziehung des Betriebsrates ist daher unbedingt anzuraten, selbst wenn es bei einzelnen Testverfahren seiner Zustimmung letztlich nicht bedarf.

4.3 Wesentliche Vertragsbedingungen für das Auftragsverhältnis zwischen Penetrationstester und Auftraggeber

4.3.1 Einordnung des Auftrags zum Penetrationstest in die Vertragstypenlehre

Bei einem Penetrationstest handelt es sich regelmäßig um eine entgeltliche Geschäftsbesorgung mit Dienstleistungscharakter. In Abgrenzung zum Werkvertrag ist lediglich die vereinbarte Leistung, nicht aber ein bestimmter wirtschaftlicher Erfolg geschuldet.

4.3.2 Allgemeine Geschäftsbedingungen

Verwendet der Auftragnehmer allgemeine Geschäftsbedingungen, so müssen diese wirksam in den Vertrag einbezogen worden sein. Voraussetzung dafür ist, dass sie dem Auftraggeber zur Kenntnis gegeben wurden und der Auftraggeber mit ihrer Geltung einverstanden ist.

4.3.3 Vertragsgegenstand

Neben dem Zweck des Penetrationstests sind Art und Umfang der einzusetzenden Mittel und Techniken zwischen den Parteien vertraglich festzuhalten.

Wesentliche Elemente des Vertragsgegenstands sind insbesondere:

- Zielsetzung des Penetrationstests

  Es sollte aus der vertraglichen Regelung klar hervorgehen, welches Ziel die auftraggebende Organisation mit der Durchführung des Penetrationstests verfolgt. Die gängigsten Zielsetzungen, die dabei in Frage kommen, sind:

  - Erhöhung der Sicherheit der technischen Systeme,
  - Identifikation von Schwachstellen als Entscheidungskriterium (z. B. für Investitionen oder die Eignung von Produkten)
  - Erlangen einer Zertifizierung/Bestätigung eines externen Dritten,
  - Erhöhung der Sicherheit der organisatorischen/personellen Infrastruktur.

  Eine ausführliche Beschreibung der möglichen Zielsetzungen findet sich in Gliederungspunkt 3.2 „Zielsetzungen von Penetrationstests“ dieser Studie.

- Art des Penetrationstests

  Es sollte weiterhin darauf Bezug genommen werden, welche Art des Penetrationstests durchgeführt werden soll (siehe Gliederungspunkt 3.4. „Klassifikation“ dieser Studie). Dabei bieten sich folgende Klassifizierungsmerkmale an:

  - Informationsbasis (Black-Box- oder White-Box -Test)
  - Aggressivität (passiv scannend bis aggressiv)
  - Umfang (vollständig, begrenzt oder fokussiert)
  - Vorgehensweise (verdeckt oder offensichtlich)
  - Technik (Netzwerkzugang, sonstige Kommunikation, physischer Zugang, Social-Engineering)
  - Ausgangspunkt (von außen oder von innen)

Eine diesbezügliche Festlegung des Auftragnehmers schließt von Beginn an unnötige Missverständnisse und Risiken aus und stellt eine individuelle Anpassung des Penetrationstests auf die Bedürfnisse des Auftraggebers sicher. Darüber hinaus wird der Umfang der unter strafrechtlichen Gesichtspunkten präventiv zu erteilenden Einwilligung des Auftraggebers festgelegt.

- Einzusetzende und auszuschließende Techniken

  Soweit es möglich und sinnvoll erscheint, sollten auch die Einzeltechniken, die im Rahmen eines Penetrationstests Anwendung finden, näher beschrieben werden. Dabei sollten insbesondere Social-Engineering-Techniken und aktive Tests der Zutrittskontrollen erläutert werden, sofern deren Anwendung beabsichtigt ist. Da Social-Engineering-Techniken von Natur aus kritisch und evtl. unethisch sind, ist es sinnvoll, hierfür klare Rahmenbedingungen festzulegen (z. B. der Verzicht auf die Anstiftung von Mitarbeitern zu unethischem Verhalten) Bei einem aktiven Test von Zutrittskontrollen wird versucht, physische Sicherheitsmaßnahmen zu umgehen, was als Einbruch gewertet werden kann. Deshalb ist auch hier eine nähere Erläuterung der Umstände, unter denen der Test stattfinden soll, vorzunehmen.

  Wichtig ist auch der Ausschluss von Angriffstechniken, die ausdrücklich nicht zum Einsatz kommen sollen. Diese sollten ebenfalls mit einer entsprechenden Begründung im Vertrag niedergelegt werden.

4.3.4 Auftraggeber

Insbesondere im Hinblick auf die erforderliche Einwilligung zur Vornahme von potentiell schadensverursachenden Maßnahmen im Rahmen der Testdurchführung ist darauf zu achten, dass der Auftraggeber bei Vertragsunterzeichnung rechtswirksam vertreten ist. Das bedeutet, dass nur eine vertretungsberechtigte Person, d. h. z. B. bei einer Handelsgesellschaft der Geschäftsführer, ein Prokurist oder eine andere mit entsprechender Einzelvollmacht ausgestattete Person, etwa der Leiter der IT-Abteilung, den Auftrag zur Durchführung des Penetrationstests erteilen kann.

Vor der Durchführung des Penetrationstests sollte sich der Penetrationstester durch einen geeigneten Nachweis von der Vertretungsberechtigung des Vertreters des Auftraggebers überzeugen.

4.3.5 Auftragnehmer

Sofern der Auftragnehmer beabsichtigt, Subunternehmer im Rahmen der Auftragsdurchführung zu beauftragen, sollte eine entsprechende Öffnungsklausel im Vertrag enthalten sein. Da es sich um sicherheitsrelevante Bereiche handelt, wird der Auftraggeber mit einer solchen Öffnungsklausel allerdings regelmäßig nicht einverstanden sein, so dass es zweckmäßig ist, einen einzusetzenden Subunter-

nehmer bereits bei Vertragsabschluss zu benennen. Dadurch wird sichergestellt, dass ausschließlich diese Personen zur Durchführung der Prüfungshandlungen autorisiert sind. Insbesondere wenn bei dem Penetrationstest unkonventionelle Prüfungshandlungen wie Social-Engineering oder die Umgehung von physischen Sicherheitsmaßnahmen vorgesehen sind, ist die konkrete Benennung der durchführenden Personen wichtig, da hierdurch eine Absicherung beider Seiten bewirkt und Missverständnissen vorgebeugt wird.

4.3.6 Schriftformklausel

Sämtliche Vertragsbedingungen sollten schriftlich vereinbart werden. Zusätzlich sollte ausdrücklich und zwingend ein Schriftformerfordernis auch für etwaige Nebenabreden geregelt werden.

4.3.7 Pflichten des Auftraggebers

Die Mitwirkungspflichten des Auftraggebers sollten im Interesse des Penetrationstesters möglichst umfassend geregelt werden. Folgende Elemente sollten hierbei beachtet werden:

- Bereitstellung von Informationen abhängig von der Art des Penetrationstests

  Abhängig von der Art des Penetrationstests ist der Penetrationstester evtl. auf umfangreiche Informationen des Auftraggebers angewiesen. Beispielsweise werden bei einem White-Box-Test Informationen über DNS-Namen, IP-Adressen, Sicherheitsleitlinien, Systemkonfigurationen, Firewallregeln, Eskalationsprozeduren etc. benötigt. Der Penetrationstester sollte deshalb vor Vertragsabschluss eine Auflistung der notwendigen Informationen dem Auftraggeber zukommen lassen und im Vertrag vereinbaren, dass die erforderlichen Informationen zeitgerecht, vollständig und richtig zur Verfügung gestellt werden.

- Information von möglicherweise betroffenen Dritten

  Bei einem Penetrationstest werden wie bei normalem Datenverkehr über öffentliche Netze auch Systeme von Dritten (z. B. Router eines Providers, Webserver eines Hosters) genutzt. Da nicht mit ausreichender Sicherheit eine Beeinträchtigung des ordnungsmäßigen Betriebes dieser Systeme ausgeschlossen werden kann, ist es sinnvoll, einen evtl. betroffenen Dritten vorab über den geplanten Penetrationstest zu informieren. Es bietet sich dabei an, diese Informationspflicht dem Auftraggeber zu übertragen, da dieser den Kreis der möglicherweise betroffenen Dritten am besten abschätzen kann.

- Schutzmaßnahmen für unvorhersehbare Systemausfälle

  Da es nicht völlig ausgeschlossen werden kann, dass im Rahmen eines Penetrationstests Systeme derart beeinträchtigt werden, dass ein Datenverlust auftritt, sollte der

Auftraggeber in seinem eigenen Sinne dazu verpflichtet werden, Datensicherungen der gefährdeten und relevanten Systeme anzufertigen, soweit dies nicht schon im Rahmen der Erfüllung der Vorschriften der GoBS der Fall ist. Durch eine Datensicherung wird die Wiederherstellbarkeit der Daten im Bedarfsfall gewährleistet und somit die möglichen negativen Folgen eines Datenverlustes abgemildert.

4.3.8 Pflichten des Auftragnehmers

Im Interesse des Auftraggebers sollten dem Auftragnehmer folgende Pflichten auferlegt werden:

- Verschwiegenheit

  Ein Penetrationstester erhält möglicherweise im Verlauf eines Penetrationstests Kenntnis von hochsensiblen Informationen über Schwachstellen innerhalb des Netzwerks des Auftraggebers. Diese Informationen dürfen Dritten nicht zugänglich gemacht werden, um die Gefährdungssituation des Auftraggebers nicht zu erhöhen. Der Auftragnehmer sollte deshalb zur Verschwiegenheit über die ihm zur Verfügung gestellten Informationen und den im Verlauf des Penetrationstests bekannt werdenden Sachverhalte verpflichtet werden.

- Einhaltung lizenzrechtlicher Vorschriften

  Der Auftragnehmer sollte für die Einhaltung der lizenzrechtlichen Vorschriften beim Einsatz von kommerziellen Sicherheitstools verantwortlich sein. Da die Lizenzgebühren für den Einsatz von Sicherheitstools üblicherweise dem Auftraggeber weiterbelastet werden, sollte die Aufgliederung dieser Lizenzgebühren dem Auftraggeber gegenüber transparent gemacht werden.

- Dokumentation der Prüfungshandlungen und der Ergebnisse

  Die Art und der Umfang der Dokumentation der durchzuführenden Prüfungshandlungen und deren Ergebnisse sollten im Vertrag festgelegt werden. Der Auftragnehmer sollte dazu verpflichtet werden, seine Prüfungshandlungen genau zu dokumentieren. Damit wird sichergestellt, dass im Falle eines Schadens die Nachvollziehbarkeit der angewandten Techniken gewährleistet ist. Darüber hinaus ist die Form der Ergebnisdarstellung (Bericht, Präsentation, Reports und Analysen der eingesetzten Sicherheits-Tools) zu vereinbaren.

- Allgemeine Sorgfaltspflichten

  Der Penetrationstester hat die allgemeinen Sorgfaltspflichten bei der Ausübung seiner Prüfungshandlungen zu beachten. Beispielsweise wäre es grob fahrlässig, wenn ein Penetrationstester „versehentlich“ durch die Verwechslung eines DNS-Namens die

Systeme eines unbeteiligten Dritten attackieren würde. Ein Hinweis, dass der Penetrationstester bei der Durchführung seiner Tätigkeit im Hinblick auf eventuelle Schadensverursachung angemessene Sorgfalt anzuwenden hat, sollte daher als Vertragsbestandteil aufgeführt werden.

4.3.9 Auftragsdurchführung

Es sollte ein Anfangs- und Enddatum des Auftrags festgelegt werden. Innerhalb dieses Zeitraumes ist der Penetrationstest zu erbringen. Damit wird sichergestellt, dass über diesen Zeitraum hinausgehende Penetrationsversuche klar als tatsächliche Angriffe eines Dritten identifiziert werden können. Missverständnisse werden dadurch ausgeschlossen. Dabei ist zu beachten, dass der Penetrationstester nur in dem vereinbarten Zeitraum zur Durchführung seiner Tests autorisiert ist.

4.3.10 Sonderkündigungsrecht

Es können während der Dauer des Penetrationstests Umstände eintreten, die eine Fortführung des Penetrationstests verhindern (beispielsweise der Absturz eines kritischen Systems, bei dem langwierige manuelle Aufräumarbeiten durchzuführen sind). Für diese Fälle kann explizit ein Sonderkündigungsrecht in den Vertrag aufgenommen werden. Darüber hinaus gelten die allgemeinen Regeln für die Kündigung von Geschäftsbesorgungsverträgen mit Dienstleistungscharakter, insbesondere § 627 Abs. 2 BGB.

4.3.11 Haftungsbeschränkung

Bei der Vereinbarung von Haftungsbeschränkungen zwischen Auftraggeber und Penetrationstester ist darauf zu achten, dass eine Haftungsbeschränkung nur innerhalb der Grenzen des AGB-Gesetzes zulässig vereinbart werden kann. Möglich ist regelmäßig eine Beschränkung der Haftung des Testers auf grobe Fahrlässigkeit und Vorsatz sowie ein Haftungsausschluss für Mangelfolge- oder indirekte Schäden, sofern nicht die schuldhafte Verletzung einer wesentlichen Vertragspflicht vorliegt.

5 Rahmenbedingungen

Bei der Durchführung von Penetrationstests existieren neben den rechtlichen Rahmenbedingungen eine Reihe von Rahmenbedingungen organisatorischer, personeller und technischer Art.

5.1 Organisatorische Voraussetzungen

Im Vorfeld eines geplanten Penetrationstests sind folgende organisatorische Voraussetzungen in Absprache mit dem Auftraggeber zu klären:

- Wer ist, abgesehen von dem Auftraggeber, direkt oder indirekt von dem Penetrationstest betroffen?

  Neben den Systemen des Auftraggebers sind häufig auch Systeme des Providers, die evtl. auch physisch beim Auftraggeber stehen, jedoch vom Provider administriert werden, von dem Penetrationstest betroffen. Um Missverständnissen vorzubeugen, sollte deshalb der Provider von dem geplanten Penetrationstest in Kenntnis gesetzt werden. Manche Prüfungsschritte, z. B. sog. DoS-Tests, können aufgrund ihres hohen Bandbreitenbedarfs oder aufgrund nicht standardkonformer Datenpakete auch zu Störungen der Netzwerkkomponenten bei den beteiligten Providern führen und sollten daher mit den Providern vorher genau abgesprochen werden.

  Sind bestimmte Funktionsbereiche ausgelagert worden (z. B. Webhosting des WWW-Servers), sind die betreffenden Systeme aus dem Penetrationstest auszuschließen Sollen die Systeme dennoch in den Penetrationstest aufgenommen werden, so muss hierfür die schriftliche Genehmigung des Systembetreibers bzw. des Outsourcing-Betreibers eingeholt werden.

  Der Auftraggeber muss aber beachten, dass die Verantwortung für die Sicherheit der IT-Systeme, z. B. für die Integrität der Daten der Buchhaltung, auch im Falle von Outsourcing bei ihm liegt und nicht einfach auf den Outsourcing-Dienstleister übertragen werden können.

- Sind haftungsrechtliche Risiken angemessen berücksichtigt?

  Der Penetrationstester sollte über eine Haftpflichtversicherung in ausreichender Deckungshöhe verfügen, um gegen mögliche Schadensersatzforderungen Dritter abgesichert zu sein. Obwohl schon im Vorfeld darauf geachtet werden sollte, mögliche Risiken für Systeme Dritter zu minimieren, lassen sich eventuelle Beeinträchtigungen fremder Systeme nicht völlig ausschließen.

- Was ist bezüglich des Durchführungszeitpunktes/-zeitraumes zu beachten?

  Durch Penetrationstests können produktive Systeme in ihrer Funktion beeinträchtigt werden. Da das Ziel eines Penetrationstests darin besteht, Schwachstellen aufzudecken, nicht jedoch den ordnungsmäßigen Geschäftsbetrieb zu gefährden, sollten die konkreten Angriffe zu einem beid-

seitig vereinbarten Zeitpunkt stattfinden. Dies ist bereits im Vorfeld bei der Planung des Penetrationstests zu berücksichtigen. Oft erstrecken sich Penetrationstests über einen längeren Zeitraum von mehreren Tagen. Es sollten auch dann Zeitpunkte gewählt werden, in denen das Zielsystem keine kritischen Verarbeitungsprozesse ausführt oder ein hohes Aufkommen von beispielsweise Online-Bestellungen bearbeiten muss. Rücksicht auf den Durchführungszeitpunkt der Angriffe kann nur im Rahmen von White Box Tests genommen werden. Bei Black Box Ansätzen steht die Information über die Kritikalität und die Beanspruchung eines Systems zu bestimmten Zeitpunkten üblicherweise nicht zur Verfügung.

- Was ist im Falle eines Systemausfalls oder eines sonstigen Notfalls zu tun?

  Für den Fall, dass es trotz Vorsicht während des Penetrationstests zu einem Systemausfall oder einem anderen Notfall, z. B. einer schwer wiegenden Systemstörung, kommt, müssen Notfallmaßnahmen vereinbart werden. Es muss mindestens festgelegt werden, wer und wann zu benachrichtigen ist, falls ein Ausfall oder eine Störung bemerkt bzw. vermutet wird. Darüberhinaus sollte definiert werden, bei welcher Störung eine Meldung erfolgen muss. Dabei kann z. B. zwischen folgenden „Störungen“ unterschieden werden:

  - Totalausfall des Systems
  - Teilausfall von bestimmten Subsystemen
  - falsche Antworten des Systems
  - stark gestiegenen Antwortzeiten des Systems
  - eingeleitete Gegenmaßnahmen bei einem verdeckten Penetrationstest
  - Angriffe Dritter gegen das System

- Welche Mitarbeiter des Auftraggebers sind durch den Penetrationstest betroffen?

  Je nach Umfang und Art des Penetrationstests werden mehr oder weniger Mitarbeiter des Auftraggebers durch den Penetrationstest betroffen sein. Bei einem auf ein Testsystem begrenzten Penetrationstest werden nur die Administratoren und die Nutzer des Testsystems durch den Penetrationstests betroffen sein können. Bei einem Test, bei dem auch Produktionssysteme untersucht werden, können im Extremfall neben den Nutzern der Systeme auch alle Mitarbeiter, die in irgendeiner Weise auf die Ergebnisse der zu testenden Systeme angewiesen sind, durch den Test betroffen bzw. in ihrer Arbeit behindert werden. Falls für den Penetrationstest auch Social-Engineering-Techniken verwendet werden sollen, so muss vereinbart werden, welche Mitarbeiter in welchem Maß im Rahmen der Tests angegangen werden dürfen.

- Welcher Aufwand ist für den Auftraggeber mit dem Penetrationstest verbunden?

  Der Auftraggeber des Penetrationstests muss ggf. damit rechnen, dass es aufgrund des Penetrationstests zu Beeinträchtigungen seiner IT-Systeme und somit zu Unregelmäßigkeiten im Geschäftsbetrieb kommen kann. Es sind daher im Vorfeld eines Penetrationstests die erforderlichen Maßnahmen zu ergreifen, um die Auswirkung potenzieller Störungen möglichst gering zu halten. Dazu zählt beispielsweise die Bereitstellung eines Mitarbeiters, der den Penetrationstest aus der Sicht des Auftraggebers überwacht und ggf. den Tester veranlassen kann, den Penetrationstest zu stoppen. Das Anfertigen von (zusätzlichen) Datensicherungen vor der Durchführung eines Penetrationstests sollte der Auftraggeber ebenfalls in Erwägung ziehen. Darüber hinaus ist es notwendig, einen Notfallplan (sofern nicht bereits vorhanden) und Eskalationsprozeduren zu verabschieden, welche ein geordnetes Vorgehen und die Einleitung von geeigneten Gegenmaßnahmen im Angriffsfall ermöglichen. Wird für den Penetrationstest der White-Box Ansatz gewählt, so müssen zusätzlich Informationen bzw. fachliche Ansprechpartner für den Penetrationstester zur Verfügung gestellt werden.

- Welcher Aufwand ist für den Tester mit dem Penetrationstest verbunden?

  Um beurteilen zu können, ob ein Dienstleister in der Lage ist, einen adäquaten Penetrationstest durchzuführen und falls ja, in welchem Rahmen sich der finanzielle Aufwand bewegt, ist zunächst der Aufwand zur Durchführung des Penetrationstests für den Penetrationstester zu quantifizieren. Folgende Aspekte sollten berücksichtigt werden:

  - Zielsetzung und Umfang des Penetrationstests

    Abhängig von der Zielsetzung des Penetrationstests legt der Tester zusammen mit dem Auftraggeber die Art des Penetrationstests und die durchzuführenden Prüfungsschritte fest. Je nach Art und Umfang des Penetrationstests kann demnach schon im Vorfeld des eigentlichen Tests eine Aussage getroffen werden, welche Ressourcen der Penetrationstester einsetzen muss (Hardware, Software, geeignete Mitarbeiter).

  - Größe der zu testenden Infrastruktur

    Die Größe der zu testenden Infrastruktur wird häufig in der Anzahl der zu testenden IP Adressen ausgedrückt. Grundsätzlich kann kein zeitlicher Wert festgelegt werden, wie lange ein Tester für den Penetrationstest eines einzelnen Systems benötigt, da dies vom Typ und der Konfiguration des Systems, von der Erfahrung und dem Einsatz des Testers und von weiteren Faktoren abhängt. Darüber hinaus spielt eine Rolle, ob die zu testenden Systeme sich in einem logischen Segment befinden, dessen Übergangspunkt zu einem öffentlichen Netz ggf. von einer zentralen Firewall geschützt wird, oder ob es sich um eine verteilte Infrastruktur mit mehreren Zugangspunkten zu öffentlichen Netzen handelt. Da

diese Faktoren nur schwer quantifizierbar sind, lässt sich daraus nur die sehr allgemeine Aussage ableiten, dass eine größere Anzahl von zu prüfenden Systemen und größere Infrastrukturen einen erhöhten Aufwand für den Penetrationstester zur Folge haben.

- Komplexität der zu testenden Infrastruktur

  Ein weiteres wesentliches Merkmal, dass den Aufwand für den Penetrationstester beeinflusst, ist die Komplexität der zu testenden Infrastruktur. Übliche Dienste, die über das Internet angeboten werden, sind der Abruf von Webseiten (HTTP), Downloadmöglichkeiten (FTP) und E-Mail Kommunikation (SMTP). Schwachstellen in Anwendungen, die diese Dienste unterstützen, sind aufgrund der weiten Verbreitung der Dienste oft bekannt und werden im Internet an vielen Stellen publiziert. Beschränkt sich ein Unternehmen oder eine Behörde auf das Angebot dieser weit verbreiteten Dienste, so kann von Infrastruktur mit niedrigem Komplexitätsgrad ausgegangen werden. Der zeitliche und personelle Aufwand bei der Durchführung eines Penetrationstests sollte deshalb vergleichsweise gering ausfallen. Werden zusätzlich umfangreiche E-Commerce Lösungen oder interaktive Anwendungen eingesetzt, ist eine längere Recherche nach Schwachstellen und ggf. eine größere Expertise bei der Ausnutzung der Schwachstellen notwendig. Dadurch muss der Penetrationstester eine längere Zeitdauer und erfahreneres Personal zur Durchführung des Penetrationstests einplanen.

5.2 Personelle Voraussetzungen

Penetrationstests sind auf die individuelle Situation des Auftraggebers abzustimmen und somit nur in begrenztem Umfang standardisierbar. Bei einem Penetrationstest kann deshalb nur bis zu einem gewissen Grad nach einem starren Muster vorgegangen werden. Deshalb sollte die Durchführung von Penetrationstests von Personen vorgenommen werden, die über langjährige Erfahrung im Bereich der IT-Sicherheit verfügen.

Im einzelnen sind insbesondere folgende Eigenschaften zur qualifizierten Durchführung von Penetrationstests notwendig:

- Kenntnisse im Bereich der Systemadministration / Betriebssyteme

  Diese Kenntnisse sind nicht nur zur Beurteilung von Schwächen in den Betriebssystemen der Zielsysteme notwendig, sondern sie erleichtern auch die Handhabung der für den Penetrationstest eingesetzten Systeme.

- Kenntnisse im Bereich TCP/IP und ggf. weiteren Netzwerkprotokollen

  Da der Datenverkehr im Internet über TCP/IP abgewickelt wird und auch sich auch im LAN TCP/IP als der Standard durchgesetzt hat, ist ein tiefgreifendes Wissen über dieses Protokoll

unerlässlich. Kenntnisse in TCP/IP sind eng mit weiteren Netzwerkkenntnissen und Kenntnissen über das OSI-Referenzmodell verknüpft.

- Kenntnisse im Bereich Programmiersprachen

  Um in der Lage zu sein, Schwachstellen in Anwendungen und Systemen auszunutzen, sind Kenntnisse in einer Programmiersprache vorteilhaft. Zwar existieren eine Reihe von vorgefertigten Tools als Skripte oder mit graphischer Benutzeroberfläche, oft können Sicherheitslücken wie Buffer Overflows o. Ä.. jedoch nur dann wirksam ausgenutzt werden, wenn der Tester über die notwendigen Programmierkenntnisse verfügt.

- Kenntnisse im Bereich von IT-Sicherheitsprodukten wie Firewalls, Intrusion-Detection-Systemen

  Da mittlerweile Sicherheitsvorkehrungen wie Firewalls oder Intrusion-Detection-Systeme einen sehr hohen Verbreitungsgrad haben, sollte der Penetrationstester die Funktionsweise dieser Sicherheitsvorkehrungen kennen und auch aktuelle Meldungen im Bereich der Sicherheitslücken von IT-Sicherheitsprodukten verfolgen. Einen Überblick über die marktgängigen Produkte im Bereich der IT-Sicherheit zu haben ist unerlässlich (für Firewalls siehe z. B. [BSI01]).

- Kenntnisse in der Handhabung von Hackertools und Schwachstellen-Scannern

  Zur Durchführung von Penetrationstest ist neben dem erforderlichen Grundlagenwissen auch Erfahrung in der Handhabung mit Hackertools und Schwachstellen-Scannern notwendig. Kenntnisse im Umgang mit diesen Tools sollten in der Praxis erworben worden sein. Aus der Vielzahl der verfügbaren Tools haben sich im Laufe der Zeit einige Produkte eine weite Verbreitung gefunden (z. B. nmap für Portscans, L0phtcrack für Windows-Passwörter). Sowohl kommerzielle Tools für die Durchführung einer effizienten Prüfung als auch frei verfügbare Werkzeuge zur Demonstration der relativ einfachen Durchführbarkeit können zum Einsatz kommen. Die Effizienz des Penetrationstests hängt aber wesentlich davon ab, wie erfahren der Penetrationstester im Umgang mit diesen Tools ist.

- Kenntnisse im Bereich von Anwendungen bzw. Anwendungssystemen

  Viele Schwachstellen liegen nicht im Bereich der Betriebssystemsoftware, sondern in den Anwendungen. Dies umfasst mit z. B. unzureichend abgesicherten Makro-Funktionen in Textverarbeitungsprogrammen über Verwundbarkeiten von Internet-Browsern mittels „Scripting“ bis hin zu sog. Buffer-Overflow-Fehlern in großen Datenbanksystemen die gesamte Bandbreite von Anwendungssystemen. Der Tester sollte daher über möglichst breite Kenntnisse von Anwendungen aller Art verfügen. Besonders wichtig sind detaillierte Kenntnisse über weit verbreiteten Anwendungen, da hier die Gefährdungen durch Hacker/Cracker im Allgemeinen besonders groß sind.

- Kreativität

Neben den hohen fachlichen Anforderungen, die ein Penetrationstester erfüllen sollte, stellt Kreativität ein wesentliches Qualifikationsmerkmal dar. Da ein qualifizierter Penetrationstest nur begrenzt nach einem starren Muster verlaufen kann, stellt sich im weiteren Verlauf eines Penetrationstests mit großer Wahrscheinlichkeit die Frage, wie an einer Stelle zu verfahren ist, an der auf den ersten Blick eine weitere Kompromittierung eines Systems nicht mehr möglich erscheint. Diese Problemstellung kann durch geschickte Kombination von gewonnenen Informationen, erkannten Schwachstellen und zur Verfügung stehenden Tools und Methoden angegangen werden. Ein kreativer Penetrationstester sollte demnach durch den Einsatz seiner Intelligenz eher in der Lage sein, einen „erfolgreichen“ Test durchzuführen, als ein Penetrationstester, der sich in der Durchführung des Tests ausschließlich auf die Ergebnisse seiner eingesetzten Tools verlässt. Die Kreativität darf dabei jedoch keinesfalls zu einem unsystematischen bzw. chaotischen Test führen, der später nicht mehr nachvollziehbar ist.

5.3 Technische Voraussetzungen

Folgende technischen Vorraussetzungen sollten erfüllt sein, damit der Penetrationstester die vorgesehenen Prüfungshandlungen durchführen kann:

- Zugang zu öffentlichen Netzen

  Der Zugang zum Internet bzw. zum öffentlichen Telefonnetz stellt eine wesentliche Voraussetzung für die Durchführung des Penetrationstests dar, da über diese Kommunikationskanäle der größte Teil der Angriffe realisiert wird. Es sollte deshalb eine ausreichend dimensionierte Internet-Anbindung zur Verfügung stehen. Dabei ist zu beachten, dass insbesondere Schwachstellen-Scanner einen hohen Bandbreitenbedarf aufweisen und deshalb die Effizienz der Durchführung des Penetrationstests u. a. von der zur Verfügung stehenden Leitungskapazität abhängt.

- Verfügbarkeit geeigneter Revisionswerkzeuge (Tools)

  Der Penetrationstester muss über die geeigneten Tools zur Durchführung der Tests verfügen. Viele dieser Tools stehen kostenlos im Internet zum Download zur Verfügung. Insbesondere im Bereich von Schwachstellen-Scannern werden (meist in Abhängigkeit von der Anzahl der zu scannenden IP-Adressen) jedoch teilweise sehr hohe Lizenzgebühren fällig. Wichtiger als möglichst viele Tools sind für einen effizienten Test die „richtigen“ Tools. Der Tester kennt Wirkung und Nebenwirkung der Tools und kann die teilweise umfangreichen Ergebnisse schnell bewerten und falsche von richtigen Aussagen unterscheiden.

- Lokales Testnetzwerk

  In einem solchen Testnetzwerk müssen die diverse Tools getestet werden, bevor sie in echten Penetrationstests eingesetzt werden. Anhand solcher Tests kann sich der Penetrationstester auch

mit der Funktionsweise und den Ergebnissen von Hackertools und Schwachstellen-Scannern vertraut machen. Darüber hinaus lassen sich bei geeigneter Konfiguration der Systeme des Testnetzwerks Schwachstellen in den Systemen testen und verifizieren.

5.4 Ethische Überlegungen

Neben den zuvor geschilderten Voraussetzungen müssen auch ethische Überlegungen vor der Durchführung von Penetrationstests in Betracht gezogen werden. Dabei ist zum einen zu klären, ob und wie weit der Einsatz von Social-Engineering-Techniken vertretbar ist. Zum anderen ist zu diskutieren, ob Schwachstellen, die als solche im Rahmen eines Penetrationstests identifiziert wurden, auch ausgenutzt werden müssen bzw. dürfen.

Zunächst soll aber noch einmal klargestellt werden, dass es sich bei einem Penetrationstest immer nur um eine Tätigkeit im Auftrag handeln darf. Ein „proaktives“ Vorgehen, d. h. ein Angriffsversuch ohne vorherige Auftragserteilung ist immer als Angriff zu werten und daher strikt abzulehnen.

5.4.1 Einsatz von Social-Engineering-Techniken

Um die Frage zu beantworten, ob der Einsatz von Social-Engineering-Techniken im Rahmen eines Penetrationstests vertretbar ist, soll zuerst dargestellt werden, warum Social-Engineering überhaupt erfolgreich ist: Die Techniken funktionieren, weil alle Menschen bestimmte Charaktermerkmale bzw. -schwächen aufweisen, die ausgenutzt werden können. Dazu zählen überaus positive Eigenschaften wie die Neigung zu Liebenswürdigkeiten, moralisches Pflichtgefühl und Hilfsbereitschaft, aber auch weniger positive Eigenschaften wie Opportunismus und die Scheu, Verantwortung zu übernehmen.

So wird z. B. nahezu jeder dem „neuen“ Chef, der selbstsicher und authentisch auftritt, auf die entsprechende Nachfrage hin vertrauliche Informationen bekannt geben. Dies geschieht einerseits aus Hilfsbereitschaft bzw. Pflichtgefühl, andererseits sicher auch aus Opportunitätsüberlegungen. Gegen diese Schwäche kann nur die wiederholte Schulung aller Mitarbeiter wirklich etwas bewirken. Man kann aber auch die These vertreten, dass Social-Engineering-Techniken erfolgreich sind, weil die eingesetzten Sicherheitsmaßnahmen unzureichend bzw. ungeeignet sind. Wenn z. B. die Passwörter automatisch vergeben werden und dabei so kompliziert sind, dass man sie sich nur schwer merken kann, werden viele User die Passwörter an „sicheren“ Plätzen notieren. Oder sie vergessen des Öfteren ihre Passwörter und fordern häufig neue Passwörter an, was ebenfalls als Ansatzpunkte für Social-Engineering nutzbar ist.

Da üblicherweise beim Einsatz von Social-Engineering-Techniken unter anderem auf Mitarbeiter des Auftraggebers direkt Einfluss ausgeübt wird, um Ihre Zuverlässigkeit bzw. ihr Sicherheitsbewusstsein zu überprüfen, könnte dies bei den Betroffenen Unbehagen auslösen. Dies könnte umso mehr der Fall

sein, wenn Social-Engineering-Techniken ohne Vorankündigung durchgeführt werden und nachher „aufgelöst“ werden.

Selbst wenn keine Informationen bzw. Namen im Ergebnisbericht des Penetrationstests genannt werden und auch mündlich gegenüber dem Auftraggeber keine personenbezogenen Informationen über das eventuelle Fehlverhalten bestimmter Mitarbeiter gegeben werden, können solche Techniken zur Verunsicherung der Mitarbeiter führen.

Aus den genannten Gründen lehnen viele Sicherheitsexperten den Einsatz von Social-Engineering im Rahmen von Sicherheitsprüfungen ab oder halten sich nur bei sehr hohen Sicherheitsanforderungen für angemessen [Kabay00].

Der Einsatz von Social-Engineering sollte also sehr gut überlegt werden. Der Tester muss den Auftraggeber in jedem Fall über die möglichen Konsequenzen von Social-Engineering aufklären und darlegen, dass diese Technik ohne vorangegangene Benutzerschulung höchstwahrscheinlich erfolgreich sein wird und dass daraus dann negative Auswirkungen auf die Mitarbeiter resultieren können.

5.4.2 Ausnutzung erkannter Schwachstellen

Meist wird vor der eigentlichen Kompromittierung des Systems eine Schwachstelle in einer Anwendung oder in dem Betriebssystem identifiziert, die sich anschließend gezielt zur Übernahme des Systems ausnutzen lässt. Hierbei stellt sich die grundsätzliche Frage, ob dieser letzte Schritt, das Ausnutzen der Schwachstelle, zur Verifikation vollzogen werden muss oder ob es genügt, auf die Existenz der Schwachstelle lediglich hinzuweisen. Diese Frage kann nur im Hinblick auf das vereinbarte Ziel und den daraus abgeleiteten Voraussetzungen beantwortet werden. Soll der Penetrationstest möglichst realitätsnah und aussagekräftig sein, so bietet es sich an, keine Einschränkungen im Bereich der Aggressivität des Vorgehens machen. Soll dagegen eine mögliche Störung der Geschäftsprozesse soweit wie möglich ausgeschlossen werden, so sollte auf das aktive Ausnutzen von Schwachstellen verzichtet werden. In diesem Fall wäre das Ergebnis des Penetrationstests der Hinweis auf eine existierende Schwachstelle, wobei jedoch der Beweis für eine erfolgreiche Penetration nicht erbracht wird.

6 Methodik für die Durchführung von Penetrationstests

In diesem Kapitel wird eine in fünf Phasen gegliederte Methodik zur Durchführung von Penetrationstests vorgestellt. Diese Methodik berücksichtigt die bisher diskutierten Aspekte und wurde im Hinblick auf eine möglichst große Allgemeingültigkeit entwickelt. Zentraler Bestandteil der Methodik ist eine strukturierte Vorgehensweise zur Durchführung von Penetrationstests, auf dessen Basis individuelle Ablaufpläne für konkrete Penetrationstests gebildet werden können.

6.1 Anforderungen an eine Methodik für die Durchführung von Penetrationstests

Die Methodik beschreibt und strukturiert die Durchführung eines Penetrationstests im Auftrag. Daher muss immer wieder eine Orientierung auf die Ziele des Auftraggebers erfolgen bzw. Sorge getragen werden, dass diese Orientierung nicht außer Acht gelassen wird. Dies bedeutet beispielsweise, dass die zur Erreichung der Ziele notwendigen Prüfungsschritte beschrieben werden, bzw. dass erläutert wird, ob die Ziele überhaupt sinnvoll mit einem Penetrationstests erreicht werden können. Des weiteren müssen Maßnahmen zur Einhaltung der rechtlichen Bestimmungen (siehe z. B. [ISACA_CH99]) und zur Beachtung von organisatorischen bzw. personellen Vorraussetzungen für die Durchführung von Penetrationstests enthalten sein. Darüber hinaus sollte eine Methodik zur Durchführung von Penetrationstests die nur begrenzt zur Verfügung stehende Zeit berücksichtigen und muss daher eine Bewertung des potenziellen Risikos bzw. einen Kosten/Nutzen Vergleich enthalten.

Für die Gruppierung der einzelnen Prüfungsschritte empfiehlt sich ein modulorientierter Ansatz, wie z. B. der des OSSTMMs [Herzog02], da ein solcher eine thematische Gruppierung der durchzuführenden Schritte innerhalb eines Penetrationstests erlaubt. Dies dient zum einen der Übersichtlichkeit, zum anderen kann so durch die Auswahl bzw. das Auslassen von bestimmten Modulen ein angemessener Penetrationstest zusammengestellt werden.

Im Rahmen eines konkreten Penetrationstests können aus wirtschaftlichen Gründen oftmals nicht alle möglichen Prüfungsmodule bearbeitet werden. Dies würde zwar eine vollständige Prüfung sicherstellen, aber auch zu einem hohen zeitlichen Aufwand führen, der u. U. nicht mit den Zielen des Auftraggebers vereinbar bzw. nicht den konkreten Sicherheitsanforderungen angemessen ist. Bei sehr hohen Sicherheitsanforderungen sollte ein möglichst vollständiger Test durchgeführt werden. D. h., dass alle bzw. die meisten Module angewendet werden müssen und dass alle Systeme des Auftraggebers mit in den Test eingeschlossen werden. Bei niedrigen Sicherheitsanforderungen können hingegen bestimmte Module ausgelassen werden und/oder nur exponierte bzw. von „außen“ sichtbare Systeme geprüft werden. Der Umfang des Penetrationstests sollte dabei durch wirtschaftliche Überlegungen bestimmt

werden. Es gilt die Kosten bzw. Risiken der Prüfungstätigkeiten mit den möglichen Kosten bzw. Risiken, die durch einen Angriff entstehen könnten, abzuwägen.

6.2 Die fünf Phasen eines Penetrationstests

Ausgehend von den oben dargestellten Überlegungen werden im Folgenden die fünf Phasen eines Penetrationstests vorgestellt. Die einzelnen Phasen laufen zeitlich nacheinander ab:

Phase 1: Vorbereitung; ohne gründliche Vorbereitung, wie z. B. eine genaue Abstimmung der Ziele des Penetrationstests, ist es sehr schwierig, die Erwartungen des Auftragsgebers zu erfüllen. Daher müssen zu Beginn eines Penetrationstests die Ziele des Auftraggebers zusammen mit ihm geklärt und definiert werden. Die Durchführung eines Penetrationstests ohne vollständige Berücksichtigung der relevanten gesetzlichen Bestimmungen wird möglicherweise strafrechtliche und/oder zivilrechtliche Konsequenzen nach sich ziehen. Deshalb muss sichergestellt sein, dass mit den Prüfungshandlungen nicht gegen gesetzliche Bestimmungen bzw. vertragliche Vereinbarungen verstoßen wird. Darüber hinaus könnte der Ausfall eines Produktivsystems aufgrund nicht abgestimmter Penetrationstechniken oder nicht kommunizierter Risiken der eingesetzten Techniken Regressforderungen auslösen, weshalb das Vorgehen und die daraus resultierenden Risiken besprochen und dokumentiert werden müssen.

Die vereinbarten Details sollten, soweit möglich schriftlich in einem Vertrag festgehalten werden.

Phase 2: Informationsbeschaffung und –auswertung; nachdem Ziele, Umfang, Vorgehen, Notfallmaßnahmen, etc. unter Berücksichtigung der rechtlichen bzw. organisatorischen Aspekte sowie der sonstigen Voraussetzungen definiert worden sind, kann mit der Sammlung von Informationen über das Ziel begonnen werden. Diese Phase wird auch als passiver Penetrationstest bezeichnet. Ziel ist es, eine möglichst komplette und detaillierte Übersicht über die installierten Systeme inklusive der potenziellen Angriffspunkte bzw. der bekannten Sicherheitsmängel zu erlangen. Je nach Anzahl der zu untersuchenden Rechner bzw. nach Größe des zu untersuchenden Netzwerkes können die Prüfungsschritte mitunter eine sehr lange Zeit benötigen. Soll z. B. ein Class-C Netzwerk (256 mögliche IP-Adressen) hinter einer Firewall komplett getestet werden, so kann ein vollständiger Portscan (alle 65536 Ports) je nach Einstellung mehrere Wochen dauern. Diese langen Prüfungsschritte laufen zwar größtenteils automatisch ab, trotzdem muss der entsprechende Zeitbedarf bei der Planung berücksichtig werden. So kann der Aufwand für einen Penetrationstest z. B. 20 Aufwandstage betragen, die Dauer bei dem o. g. Fall aber mehrere Wochen.

Phase 3: Bewertung der Informationen / Risikoanalyse; ein erfolgreiches, nachvollziehbares und vor allem ein wirtschaftlich effizientes Vorgehen muss die gesammelten Informationen

analysieren und bewerten, bevor die zum Teil sehr zeitaufwendigen Prüfungsschritte zum aktiven Eindringen durchgeführt werden. In die Bewertung müssen die vereinbarten Ziele des Penetrationstests, die potenzielle Gefährdung der Systeme und der geschätzte Aufwand für das Evaluieren der potenziellen Sicherheitsmängel für die nachfolgenden aktiven Eindringversuche einfließen. Anhand dieser Bewertung werden dann die Angriffsziele für Phase 4 ausgewählt. So können z. B. aus der Liste der identifizierten Systeme für das weitere Vorgehen nur solche ausgewählt werden, für die aufgrund ihrer Konfiguration bzw. der identifizierten Applikationen/Dienste potenzielle Schwachstellen bekannt sind oder solche, bei denen ein Tester beispielsweise über besonders detaillierte Kenntnisse verfügt.

Bei einem Penetrationstest, bei dem schon für Phase 2 eine genau definierte Anzahl von Zielsystemen vereinbart wurde, bedeutet die Auswahl faktisch eine Reduktion der Zielsysteme für Phase 4.

Die vorgenommenen Einschränkungen müssen ausführlich dokumentiert und begründet werden, da sie zwar einerseits zu der erwünschten Effizienzsteigerung, andererseits aber auch zu einer Einschränkung der Aussagekraft des Penetrationstests führen, welche klar zum Auftraggeber kommuniziert werden sollte.

Phase 4: Aktive Eindringversuche; schließlich werden die ausgewählten Systeme aktiv angegriffen. Diese Phase birgt das größte Risiko innerhalb eines Penetrationstests und sollte daher mit der nötigen Sorgfalt durchgeführt werden. Hier zeigt sich aber erst, inwieweit die vermeintlichen Schwachstellen, die im Rahmen der Informationsbeschaffung identifiziert wurden, tatsächliche Risiken darstellen. Falls eine Verifikation der potenziellen Schwachstellen gefordert ist, muss diese Prüfungsphase durchgeführt werden. Bei Systemen, an die sehr hohe Ansprüche an die Verfügbarkeit bzw. an die Integrität gestellt werden, müssen vor Durchführung von kritischen Prüfungshandlungen, wie z. B. die Ausnutzung von Buffer-Overflow-Exploits, die möglichen Konsequenzen jeweils genau abgewogen werden.

Im Rahmen eines White-Box Test muss bei kritischen Systemen vor der Durchführung des Tests ein eventuell verfügbarer Patch installiert werden, um einen Ausfall zu verhindern. Die Prüfung wird dann wahrscheinlich keine Schwachstelle feststellen können, dafür aber die Sicherheit des Systems dokumentieren. Im Gegensatz zu einer Hacking Attacke ist der Penetrationstest jedoch nicht abgeschlossen, sondern wird fortgeführt.

Phase 5: Abschlussanalyse; neben den Aufzeichnungen der einzelnen Prüfungsschritte sollte der Abschlussbericht auch eine Bewertung der gefundenen Schwachstellen in Form der potenziellen Risiken sowie Empfehlungen zur Kompensation der Schwachstellen bzw. der Risiken enthalten. Der Bericht muss in jedem Fall die Nachvollziehbarkeit der Tests und der dadurch offen gelegten Schwachstellen garantieren. Die Feststellungen und die daraus resultierenden

Risiken für die IT-Sicherheit sollten nach Beendigung der Prüfungshandlungen in einem Abschlussgespräch mit dem Auftraggeber ausführlich besprochen werden.

6.3 Vorgehensweise

In Abbildung 2 ist die Vorgehensweise für die fünf Phasen eines Penetrationstests dargestellt. Die Dokumentation des Penetrationstests soll parallel während der Phasen 1 bis 5 erstellt werden und nicht erst nach bzw. während der Abschlussanalyse in Phase 5. Dies stellt sicher, dass die Prüfungsschritte und Ergebnisse aller Phasen protokolliert werden und macht damit den Penetrationstest transparent und nachvollziehbar.

Abbildung 2: Fünfphasige Vorgehensweise für Penetrationstests

Trotz des Bestrebens, die Methodik möglichst allgemeingültig zu gestalten, wird es in der Praxis eventuell zu Situationen kommen, die ein Abweichen von der vorgestellten Vorgehensweise notwendig machen können. In diesen Fall müssen die Schritte, die von der dargestellten Vorgehensweise abweichen, gesondert dokumentiert und begründet werden.

6.4 Module für die Prüfungshandlungen

Die oben vorgestellte Vorgehensweise enthält keine expliziten Prüfungshandlungen, sondern nur das Ausführen von I- und E-Modulen: Die verschiedenen Prüfungshandlungen, die im Rahmen eines Penetrationstests durchgeführt werden können, wurden – in Anlehnung an das OSSTMM [Herzog02] – in Module zusammengefasst. Zugriff auf die zu prüfenden Objekte erfolgt nur in Phase 2 – „Informationsbeschaffung“ und in Phase 4 – „Aktive Eindringversuche“. Entsprechend wurden die Module in zwei Klassen, **I-Module** für die Informationsbeschaffung und **E-Module** für die Eindringversuche, aufgeteilt. Weiterhin wurden die einzelnen Module so eingeteilt, dass die enthaltenen Schritte alle zu den gleichen Werten der Klassifizierungskriterien von Penetrationstests gehören. So wurde z. B. die Durchführung von Portscans in ein Modul zur Durchführung verdeckter Portscans und ein Modul für offensichtliche Portscans und die Prüfung von Firewalls in Module zur Prüfung von außen und innen aufgeteilt.

6.4.1 Module zur Informationsbeschaffung

In Tabelle 1 ist eine Liste der Module I 1 bis I 22 zur Informationsbeschaffung angegeben. Die in den Modulen enthaltenen Prüfungsschritte sind in 6.5.1 beschrieben und die etwaige Zuordnung zu OSSTMM Modulen sind im Anhang (A.6.1) aufgelistet.

Nr.	*Modulbezeichnung*
I 1	Auswertung öffentlich zugänglicher Daten
I 2	Verdeckte Abfragen von Netzwerkbasisinformationen
I 3	Offensichtliche Abfragen von Netzwerkbasisinformationen
I 4	Verdeckte Durchführung von Portscans
I 5	Offensichtliche Durchführung von Portscans
I 6	Identifikation von Anwendungen
I 7	Identifikation von Systemen
I 8	Verdeckte Identifikation der Router
I 9	Offensichtliche Identifikation der Router
I 10	Verdeckte Identifikation der Firewalls
I 11	Offensichtliche Identifikation der Firewalls
I 12	Recherche nach Schwachstellen
I 13	Identifikation von Anwendungsschnittstellen
I 14	Sammlung von Informationen für Social-Engineering
I 15	Sammlung von Informationen für computerbasiertes Social-Engineering
I 16	Sammlung von Informationen für persönliches Social-Engineering
I 17	Überprüfung der drahtlosen Kommunikation (nur scannend)
I 18	Test der Telefonanlage (Identifikation)
I 19	Test des Voicemailsystems (Identifikation)
I 20	Test des Faxsystems (Identifikation)
I 22	Identifikation von Zutrittskontrollen
I 21	Analyse der physischen Umgebung
I 22	Identifikation von Zutrittskontrollen

Tabelle 1: Übersicht der Module zur Informationsbeschaffung

6.4.2 Module für aktive Eindringversuche

In Tabelle 2 ist eine Liste der Module E 1 bis E 23 für die aktiven Eindringversuche angegeben. Die in den Modulen enthaltenen Prüfungsschritte sind in 6.5.2 beschrieben und die etwaige Zuordnung zu OSSTMM Modulen sind im Anhang (A.6.2) aufgelistet.

Nr.	*Modulbezeichnung*
E 1	Verdeckte Verifikation tatsächlicher Schwachstellen
E 2	Offensichtliche Verifikation tatsächlicher Schwachstellen
E 3	Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen
E 4	Verdeckter Test der Router
E 5	Offensichtlicher Test der Router
E 6	Test von Vertrauensbeziehungen zwischen Systemen
E 7	Verdeckter Test der Firewall von außen
E 8	Offensichtlicher Test der Firewall von außen
E 9	Beidseitiger Test der Firewall
E 10	Test des IDS-Systems
E 11	Abhören von Passwörtern
E 12	Test von Passwörtern
E 13	Test von „Denial-of-Service“ Anfälligkeit
E 14	Computerbasiertes Social-Engineering
E 15	Direktes, persönliches Social-Engineering mit physischem Zutritt
E 16	Indirektes, persönliches Social-Engineering ohne physischen Zutritt
E 17	Überprüfung der drahtlosen Kommunikation
E 18	Test der administrativen Zugänge zur Telefonanlage
E 19	Test des Voicemailsystems
E 20	Test der administrativen Zugänge zum Faxsystems
E 21	Test von Modems
E 22	Aktiver Test der Zutrittskontrollen
E 23	Überprüfung der Eskalationsprozeduren

Tabelle 2: Übersicht der Module für aktive Eindringversuche

6.4.3 Erweiterbarkeit

Sollten zukünftige Entwicklungen weitere, bisher nicht berücksichtigte Prüfungsschritte erfordern, so kann die Liste der Module erweitert werden. Dabei ist zu beachten, dass alle durchzuführenden Schritte in einem neuen Modul den gleichen Klassifizierungskriterien zugeordnet werden können. Sonst kann das Modul aufgrund des Ausschlussprinzips nicht in die Methodik integriert werden.

6.4.4 Ausschlussprinzip

Die Auswahl der Module erfolgt nicht nach einem positiven Auswahlprinzip, sondern nach einem negativen Ausschlussprinzip. Anhand der gewählten Klassifikation werden die Module bei den Tests ausgelassen, die aufgrund der gewählten Vorgehensweise nicht durchgeführt werden können. Wird ein Modul nicht ausgeschlossen, so müssen die enthaltenen Prüfungshandlungen durchgeführt werden, was zur Gewährleistung eines möglichst vollständigen Penetrationstests beiträgt. Falls ein Modul aus anderen Gründen ausgeschlossen werden soll, so müssen die Gründe hierfür erläutert und dokumentiert werden.

Nachdem die Ziele des Penetrationstests vereinbart worden sind, wird unter Berücksichtigung der rechtlichen und organisatorischen Aspekte der adäquate Test anhand des Klassifikationsschemas (siehe 3.4) ausgewählt. Die getroffene Klassifikation bestimmt dann über das Ausschlussprinzip, welche Module zur Informationsbeschaffung und zum aktiven Eindringen nicht ausgeführt werden dürfen. Dazu ist in

Abbildung 3 nochmals das Klassifikationsschema dargestellt, zusätzlich sind jedoch bei den gewählten Kriterien die auszuschließenden Module angegeben.

Die Wahl der Informationsbasis – White-Box oder Black-Box – hat keinen direkten Einfluss auf die Auswahl der Module. Bei einem White-Box-Test können ja nach vorliegenden Unterlagen jedoch viele Prüfungshandlungen entfallen und durch „Nachlesen“ ersetzt werden.

Abbildung 3: Ausschluss der Module durch die Klassifikation

Zur Verdeutlichung wird das Vorgehen kurz demonstriert. Soll z. B. folgender Penetrationstests durchgeführt werden:

	Kriterium	Wert	ausgeschlossene I-Module	ausg. E-Module
1.	Informationsbasis:	**Black-Box**	-	-
2.	Aggressivität:	**vorsichtig**	-	E 13
3.	Umfang:	**fokussiert**	-	-
4.	Vorgehensweise:	**verdeckt**	I 3, 5, 9, 11	E 2, 5, 8, 10, 23
5.	Technik:	**Netzwerkzugang**	I 14-22	E 14-23
6.	Ausgangspunkt:	**von außen**	-	E 9, 23

So resultiert daraus ein Ausschluss der I-Module 3, 5, 9, 11, 13-22 sowie der E-Module 2, 5, 6, 8-10, 14-23. Die übrigen Module müssen im Rahmen des Penetrationstests durchgeführt werden.

6.5 Modulbeschreibungen

6.5.1 Beschreibung der Module zur Informationsbeschaffung

In diesem Abschnitt sind die Beschreibungen der Module I 1 bis I 22 zur Informationsbeschaffung aufgeführt. Dazu sind für jedes Modul eine kurze Beschreibung, die erwarteten Ergebnisse, die Voraussetzungen, die durchzuführenden Prüfungsschritte sowie die damit verbundenen Risiken angegeben.

I 1. Auswertung öffentlich zugänglicher Daten	
Es wird versucht, so viele Informationen wie möglich über die Zielorganisation in Erfahrung zu bringen. Insbesondere wird versucht, an Informationen über das Unternehmen, die Mitarbeiter und über die eingesetzten Technologien zu gelangen.	
Erwartete Ergebnisse:	**erledigt**
• Profil des Unternehmen	☐
• Profil der Mitarbeiter	☐
• Überblick über die von der Organisation eingesetzten Technologien	☐
• Überblick über Partnerschaften und Strategien der Organisation	☐
Voraussetzungen:	
Keine	
Prüfungsschritte:	**Aufwand**
• Recherche nach Informationen auf der Homepage der Organisation	gering
• Recherche in öffentlichen Datenbanken	gering
• Recherche in Newsgroups nach relevanten Informationen	mittel
Risiken:	
Keine	

I 2. Verdeckte Abfragen von Netzwerkbasisinformationen	
Es werden die grundlegenden Informationen über das zu überprüfende Netz als Basis für einen Penetrationstest durch unauffällige bzw. verdeckte Abfragen in Erfahrung gebracht.	
Erwartete Ergebnisse:	**erledigt**
• Domain-Namen	☐
• IP-Adressbereiche	☐
• Hostnamen	☐
• IP-Adressen	☐
• Beschreibung der Server-Funktionen	☐
• ISP-Informationen	☐
• Ansprechpartner (Admin-C)	☐
Voraussetzungen:	
IP-Adresse bzw. IP-Range oder Domain- bzw. Servernamen	
Prüfungsschritte:	**Aufwand**
• Abfrage von öffentlichen Datenbanken (Whois, Ripe, Arin)	gering
• Abfrage von Name-Servern (Vorsicht: Versuch eines Zonentransfers könnte erkannt werden)	mittel
• Untersuchung der Informationen von E-Mail Headern	gering
• Untersuchung des HTML-Informationen der angebotenen Webseiten auf interne Links oder Kommentare	mittel
• Untersuchung von Newsgroups auf Postings von Mitarbeitern der Zielorganisation	gering
• Untersuchung von Stellenanzeigen der Zielorganisation auf Informationen zum IT-Umfeld	gering

Risiken:
Keine

I 3. Offensichtliche Abfragen von Netzwerkbasisinformationen	
Es werden die grundlegenden Informationen über das zu überprüfende Netz als Basis für einen Penetrationstest in Erfahrung gebracht.	
Erwartete Ergebnisse:	**erledigt**
• Domain-Namen	☐
• IP-Adressbereiche	☐
• Hostnamen	☐
• IP-Adressen	☐
• Beschreibung der Server-Funktionen	☐
• ISP-Informationen	☐
• Ansprechpartner (Admin-C)	☐
Voraussetzungen:	
IP-Adresse bzw. IP-Range oder Domain- bzw. Servernamen	
Prüfungsschritte:	**Aufwand**
• Abfrage von öffentlichen Datenbanken (Whois, Ripe, Arin)	gering
• Abfrage von Name-Servern inkl. Versuch eines „Zone-Transfers“	gering
• Pingscan über die IP-Range, benachbarte IP-Adresse und übliche Hostnamen	gering
• Untersuchung der Informationen von E-Mail Headern	gering
• Untersuchung der angebotenen Webseiten auf interne Links oder Kommentare	mittel
• Untersuchung von Newsgroups auf Postings von Mitarbeitern der Zielorganisation	gering
• Untersuchung von Online-/Offline-Stellenanzeigen der Zielorganisation auf Informationen zum IT-Umfeld	gering

Risiken:
Keine

I 4. Verdeckte Durchführung von Portscans	
Es werden alle identifizierten Geräte einem unauffälligen bzw. verdeckten Portscan unterzogen um festzustellen, welche Dienste das jeweilige Gerät mit welchem Betriebssystem anbietet.	
Erwartete Ergebnisse:	**erledigt**
• Informationen über angebotene Dienste des Geräts	☐
• Identifizierung des Betriebssystems	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen.	
Prüfungsschritte:	**Aufwand**
• Durchführung eines Portscans, der sich nicht bzw. nur schwierig entdecken lässt. Dies kann z. B. mit Hilfe geeigneter Parameter bei dem Einsatz von Portscanning–Tools oder durch lange Pausen zwischen den einzelnen Abfragen erreicht werden.	mittel
Risiken:	
Der Portscan könnte entdeckt werden.	

I 5. Offensichtliche Durchführung von Portscans	
Es werden alle identifizierten Geräte einem Portscan unterzogen um festzustellen, welche Dienste das jeweilige Gerät mit welchem Betriebssystem anbietet.	
Erwartete Ergebnisse:	**erledigt**
• Informationen über angebotene Dienste des Geräts	☐
• Identifizierung des Betriebssystems	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen.	
Prüfungsschritte:	**Aufwand**
• Durchführung eines normalen Portscans.	mittel
Risiken:	
keine.	

I 6. Identifikation von Anwendungen	
Es wird versucht, über das Internet erreichbare Anwendungen und Dienste zu identifizieren.	
Erwartete Ergebnisse:	**erledigt**
• Identifikation von angebotenen Serverdienste (z. B. HTTP, FTP, NNTP)	☐
• Identifikation von angebotenen Anwendungen (z. B. Web-Mail, Onlinebanking, E-Commerce Software)	☐
Voraussetzungen:	
Ergebnisse aus einem zuvor durchgeführten Portscan.	
Prüfungsschritte:	**Aufwand**
• Auswertung der Ergebnisse des Portscans	mittel
• Ermittlung der öffentlich zur Verfügung gestellten Internet-Anwendungen, wie z. B. Online-Banking	gering
Risiken:	
Keine	

I 7. Identifikation von Systemen	
Es wird versucht, Informationen über das Betriebssystem, den Patchlevelstand und die Hardware der Systeme zu ermitteln.	
Erwartete Ergebnisse:	**erledigt**
• Informationen über das eingesetzte Betriebssystem	☐
• Information über eingesetzte Patchlevelstände	☐
• Information über eingesetzte Hardware	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen.	
Prüfungsschritte:	**Aufwand**
• Durchführung eines Portscans mit Systemerkennung // IP-Paket-Analyse	mittel
• Auswertung von Banner-Informationen	mittel
Risiken:	
Die überprüften Systeme könnte abstürzen oder in ihrer ordnungsmäßigen Funktionsfähigkeit beeinträchtigt werden.	

I 8. Verdeckte Identifikation der Router	
Es wird versucht, die eingesetzten Router, deren Funktion innerhalb des Netzwerkes, sowie das eingesetzte Betriebssystem, Hersteller und Typ der Router der Zielorganisation durch unauffällige bzw. verdeckte Abfragen zu identifizieren.	
Erwartete Ergebnisse:	**erledigt**
• IP-Adresse der Router	☐
• Funktion der Router im Netzwerk	☐
• Betriebssystem, Hersteller und Typ der Router	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen. Ergebnisse der verdeckten Portscans und Systemidentifikation	
Prüfungsschritte:	**Aufwand**
• Vorsichtige Routenverfolgung durch „Trace Route“-Befehl	mittel
• Analyse der gerouteten IP-Pakete	mittel
Risiken:	
Der Identifikationsversuch der Router könnte erkannt werden.	

I 9. Offensichtliche Identifikation der Router	
Es wird versucht, die eingesetzten Router, deren Rolle innerhalb des Netzwerkes, sowie das eingesetzte Betriebssystem der Router der Zielorganisation zu identifizieren.	
Erwartete Ergebnisse:	**erledigt**
• IP-Adresse der Router	☐
• Rolle der Router im Netzwerk	☐
• Betriebssysteme der Router	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen. Ergebnisse der offensichtlichen Portscans und Systemidentifikation	
Prüfungsschritte:	**Aufwand**
• Routenverfolgung durch „Trace Route“-Befehl	mittel
• Analyse der gerouteten IP-Pakete	mittel
Risiken:	
Keine	

I 10. Verdeckte Identifikation der Firewalls	
Es wird versucht, die Firewalls zu identifizieren: o Art bzw. Aufbau (Packet Filter, Dual- oder Single-Homed, Application Gateway, etc.) o Typ (Hersteller, Version, Konfigurationszugänge, etc.) o Konfiguration (offene Ports, offene Protokolle, etc.)	
Erwartete Ergebnisse:	**erledigt**
• IP-Adressen und/oder DNS-Namen der Firewall-Komponenten (Firewall-Hosts, Applikation Gateway, etc.)	☐
• Betriebssysteme der Firewalls	☐
• IP-Adressen weiterer Bestandteile der Firewall-Konfiguration (innerer und äußerer Router)	☐
• Typ und Patchlevel der Firewall-Software	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen, Ergebnisse der verdeckten Portscans	
Prüfungsschritte:	**Aufwand**
• Banner-Lookup der Firewall-Komponenten	gering
• Direkter Portscan auf die Firewalls	mittel
• Routenverfolgung durch „Trace Route“-Befehl	mittel
Risiken:	
Der Identifikationsversuch der Firewalls könnte erkannt werden.	

I 11. Offensichtliche Identifikation der Firewalls	
Es wird versucht, die Firewalls zu identifizieren: o Art bzw. Aufbau (Packet Filter, Dual- oder Single-Homed, Application Gateway, etc.) o Typ (Hersteller, Version, Konfigurationszugänge, etc.) o Konfiguration (offene Ports, offene Protokolle, etc.)	
Erwartete Ergebnisse:	**erledigt**
• IP-Adressen und/oder DNS-Namen der Firewall-Komponenten (Firewall-Hosts, Applikation Gateway, etc.)	☐
• Betriebssysteme der Firewalls	☐
• IP-Adressen weiterer Bestandteile der Firewall-Konfiguration (innerer und äußerer Router)	☐
• Typ und Patchlevel der Firewall-Software	☐
Voraussetzungen:	
Kenntnis von Netzwerkbasisinformationen, Ergebnisse der offensichtlichen Portscans	
Prüfungsschritte:	**Aufwand**
• Banner-Lookup der Firewall-Komponenten	gering
• Direkter Portscan auf die Firewalls	mittel
• Routenverfolgung durch „Trace Route“-Befehl	mittel
Risiken:	
Keine	

I 12. Recherche nach Schwachstellen	
Die bisher gewonnenen Informationen (offene Ports, Anwendungen, Betriebssysteme) werden systematisch nach Schwachstellen ausgewertet. Dabei kommen verschiedene Hilfsmittel zum Einsatz.	
Erwartete Ergebnisse:	**erledigt**
• Ergänzte Liste der Patchlevel von Systemen und Anwendungen	☐
• Liste der potenziellen Schwachstellen	☐
Voraussetzungen:	
Umfangreiche Kenntnisse über offene Ports, angebotene Dienste, eingesetzte Anwendungen und verwendete Betriebssysteme.	
Prüfungsschritte:	**Aufwand**
• Einsatz von aktuellen Schwachstellenscannern (siehe A.7)	mittel
• Abfrage aktueller Schwachstellendatenbanken (siehe A.7)	mittel
• Durchsuchen von Mailinglisten/Underground FTP-Archiven, IRC Servern und Newsgroups zum Thema Hacking/Exploits.	hoch
Risiken:	
Durch den Einsatz von Schwachstellenscannern können die überprüften Geräte oder die genutzten Netzkomponenten abstürzen oder in anderer Weise negativ beeinflusst werden.	

I 13. Identifikation von Anwendungsschnittstellen	
Es werden die identifizierten, über das Internet erreichbaren Anwendungsschnittstellen, insbesondere zwischen eigenentwickelten Systemen, auf potentielle Schwachstellen untersucht. Hierbei kann es sich sowohl um Anwendungen der DMZ handeln, die u. U. über eine Schnittstelle auf Anwendungen im Unternehmensnetzwerk zugreifen können (z. B. Zugriff auf das System bei Online-Transaktionen), als auch um Anwendung innerhalb des Unternehmensnetzwerks.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung von möglichen Schwachstellen in Anwendungsschnittstellen (z. B. Webserver, ERP-System,).	☐
• Erkenntnisse über die ggf. vorhandenen Schnittstellen zwischen den verschiedenen Anwendungen.	☐
Voraussetzungen:	
Informationen über eingesetzte Anwendungen und Systeme, Ergebnisse der Portscans	
Prüfungsschritte:	**Aufwand**
• Untersuchung der angebotenen Dienste auf der Homepage, wie beispielsweise Datenbankabfragen etc. auf mögliche Schwachstellen.	hoch
Risiken:	
Keine	

I 14. Sammlung von Informationen für Social-Engineering	
Beschaffung von Informationen für Social-Engineering, die von der Zielorganisation wissentlich oder unwissentlich zur Verfügung gestellt werden.	
Erwartete Ergebnisse:	**erledigt**
• Identifizierung der relevanten Abteilungen	☐
• Auflistung von Personen, die in den relevanten Abteilungen arbeiten	☐
• Namen, Funktionsbeschreibungen, E-Mail Adressen möglicher Zielpersonen	☐
• Organisationscharts der Zielorganisation mit den verschiedenen Hierarchieebenen und Führungspositionen (Abteilungsleitern etc.)	☐
• Aufbau der E-Mail-Adressen, internen Mailinglisten und typische Absender von internen Mailings	☐
Voraussetzungen:	
Firmennamen bzw. Name der Einrichtung	
Prüfungsschritte:	**Aufwand**
• Analyse der Informationen auf der Webseite der Zielorganisation	gering
• Analyse der Informationen aus Printmedien oder Datenbanken	hoch
• Recherche in Newsgroups nach E-Mail Adressen von Mitarbeitern und Anwendungen der Zielorganisation, die in Postings veröffentlicht wurden.	mittel
Risiken:	
Keine	

I 15. Sammlung von Informationen für computerbasiertes Social-Engineering	
Beschaffung von Informationen für computerbasiertes Social-Engineering, die von der Zielorganisation wissentlich oder unwissentlich zur Verfügung gestellt werden.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung von IT-Systemen und IT-Anwendungen, die in den verschiedenen Abteilungen eingesetzt werden	☐
Voraussetzungen:	
Ergebnisse I 14: Informationen über Abteilungen / Personen / Organisation etc.	
Prüfungsschritte:	**Aufwand**
• Analyse der Webseite der Zielorganisation nach Informationen über eingesetzte Betriebssysteme und Anwendungen	gering
• Recherche von Stellenanzeigen der Organisation hinsichtlich eingesetzter IT-Systeme	hoch
• Recherche in Support-Foren nach Postings von Mitarbeitern der Zielorganisation	mittel
• Identifizierung der Mail-Programme der Zielorganisation/Mitarbeiter anhand des Headers	gering
Risiken:	
Keine	

I 16. Sammlung von Informationen für persönliches Social-Engineering	
Beschaffung von Informationen für persönliches Social-Engineering, die von der Zielorganisation wissentlich oder unwissentlich zur Verfügung gestellt werden.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der Service-Firmen, die für die Zielorganisation tätig sind	☐
• Auflistung der wichtigen Kunden der Zielorganisation	☐
• Informationen über den Sitz der verschiedenen Abteilungen innerhalb der Gebäude	☐
Voraussetzungen:	
Ergebnisse I 14: Informationen über Abteilungen / Personen / Organisation etc.	
Prüfungsschritte:	**Aufwand**
• Analyse der Kontaktinformationen auf der Webseite der Zielorganisation	gering
• Analyse der Kontakt- bzw. Kundeninformationen aus Printmedien oder Datenbanken	mittel
• Beobachtung des Gebäudes der Zielorganisation	hoch
• Ermittlung von Service-Firmen durch telefonische Nachfragen	mittel
Risiken:	
Keine	

I 17. Überprüfung der drahtlosen Kommunikation (nur scannend)	
Es wird überprüft, ob ein WLAN betrieben wird. Falls die Existenz eines WLANs verifiziert werden kann, werden die wichtigsten Eckdaten erhoben.	
Erwartete Ergebnisse:	**erledigt**
• Verifikation der Existenz eines WLAN	☐
• Identifikation des Typs und der Zugangspunkte zum WLAN	☐
• Art des Verbindungsaufbaus (authentifiziert oder unauthentifiziert)	☐
• Geographische Ausdehnung des WLAN	☐
• Überprüfung des Einsatzes und Art der Verschlüsselungstechnologie	☐
Voraussetzungen:	
Keine	
Prüfungsschritte:	**Aufwand**
• Versuch des Verbindungsaufbaues mit dem WLAN	mittel
• Mithören des WLAN-Verkehrs	hoch
• War Walking / War Driving (Ausdehnung des WLAN ermitteln)	mittel
Risiken:	
Keine	

I 18. Test der Telefonanlage (Identifikation)	
Es wird versucht, den Typ und die Zugriffsmöglichkeiten der Telefonanlage zu identifizieren.	
Erwartete Ergebnisse:	**erledigt**
• Identifikation der Telefonanlage	☐
• Identifikation der Remote Zugänge für Wartungszwecke	☐
Voraussetzungen:	
Telefonnummernbereich	
Prüfungsschritte:	**Aufwand**
• Testanrufe an Rufnummern innerhalb des Nummernbereichs der Ziel-organisation	mittel
• Auswertung der Signale der Telefonanlage	sehr hoch
• Recherche in Produktdokumentation der Telefonanlage über voreinge-stellte Wartungszugangsnummern/Standard-Passwörtern	mittel
Risiken:	
Keine	

I 19. Test des Voicemailsystems (Identifikation)	
Es wird versucht, herauszufinden, ob ein Mailboxsystem eingesetzt wird. Wenn die Existenz eines Mailboxsystems verifiziert werden kann, werden weitere Informationen erhoben.	
Erwartete Ergebnisse:	**erledigt**
• Verifikation der Existenz eines Mailboxsystems	☐
• Verifikation der Möglichkeit des Abrufens der Mailbox über das öffentliche Telefonnetz	☐
• Auflistung der identifizierten abrufbaren Mailboxen	☐
Voraussetzungen:	
Keine	
Prüfungsschritte:	**Aufwand**
• Testanrufe an Rufnummern innerhalb des Nummernbereichs der Ziel-organisation	mittel
• Recherche in der Produktdokumentation der Telefonanlage über Einzelheiten des Mailboxsystems.	mittel
Risiken:	
Keine	

I 20. Test des Faxsystems (Identifikation)	
Es wird versucht, herauszufinden, welche Faxgeräte von der Zielorganisation eingesetzt und von welchen Systemen diese ggf. gesteuert werden.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der Faxgeräte	☐
• Auflistung der Systeme, die evtl. Faxgeräte steuern und deren Betriebssystem	☐
Voraussetzungen:	
Telefonnummernbereich(e)	
Prüfungsschritte:	**Aufwand**
• Testanrufe an Rufnummern innerhalb des Nummernbereichs der Ziel-organisation	mittel
• Einsatz eines War-Dialers mit Systemerkennungskomponente	hoch
• Recherche in der Produktdokumentation der Faxgeräte über evtl. Fernwartungszugänge	mittel
Risiken:	
Angriff könnte erkannt werden.	

I 21. Analyse der physischen Umgebung	
Es wird die Umgebung des Werksgeländes hinsichtlich organisatorischer Abläufe und Schnittstellen nach außen untersucht.	
Erwartete Ergebnisse:	**erledigt**
• Gebäude- / Umgebungsplan	☐
• Auflistung einsehbarer Räume	☐
• Auflistung potentiell abhörbarer Räume (mittels elektro-akustischer oder optischer Methoden)	☐
• Auflistung organisatorischer Abläufe (Lieferungen, etc.)	☐
Voraussetzungen:	
Keine	
Prüfungsschritte:	**Aufwand**
• Beobachtung des Werksgeländes und der Umgebung	mittel
• Beobachtung der Abläufe bei Lieferung, Reinigung, Besuch etc.	hoch
Risiken:	
Keine	

I 22. Identifikation von Zutrittskontrollen	
Es werden die Zutrittskontrollen zum Werksgelände und zu kritischen Bereichen (z. B. Rechenzentrum, Serverräume) und potenzielle Umgehungsmöglichkeiten identifiziert.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der Zutrittsmöglichkeiten	☐
• Auflistung der installierten Zutrittskontrollen	☐
• Authentifizierungsverfahren für Organisationsangehörige und Gäste	☐
• Umgehungsmöglichkeiten für die installierten Schutzmaßnahmen	☐
Voraussetzungen:	
Gebäude- bzw. Lagepläne	
Prüfungsschritte:	**Aufwand**
• Beobachtung des Werksgeländes und der Umgebung	mittel
• Analyse der Zutrittskontrollen auf Wirksamkeit bzw. Umgehungsmöglichkeiten	hoch
Risiken:	
Keine	

6.5.2 Beschreibung der Module für aktive Eindringversuche

In diesem Abschnitt sind die Beschreibungen der Module E 1 bis E 23 für die aktiven Eindringversuche aufgeführt. Dazu sind für jedes Modul eine kurze Beschreibung, die erwarteten Ergebnisse, die Vorraussetzungen, die durchzuführenden Prüfungsschritte sowie die damit verbundenen Risiken angegeben.

E 1. Verdeckte Verifikation tatsächlicher Schwachstellen	
Es werden die identifizierten Schwachstellen auf ihr tatsächliches Gefährdungspotenzial hin untersucht, indem versucht wird, die Schwachstelle mit dem Ziel der Kompromittierung des Systems auszunutzen.	
Erwartete Ergebnisse:	**erledigt**
• Ergänzte Liste der Patchlevel von Systemen und Anwendungen	☐
• Liste der tatsächlichen Schwachstellen	☐
• Liste der potenziellen Schwachstellen, die nicht verdeckt verifiziert werden können	☐
Voraussetzungen:	
Ergebnisse I 12: Liste der potenziellen Schwachstellen	
Prüfungsschritte:	**Aufwand**
• Einsatz von aktuellen Schwachstellenscannern (siehe A.7), wobei nur solche Scans durchgeführt werden dürfen, die nicht erkannt werden können bzw. die nur schwer zu erkennen sind. Dazu ist z. B. Anzahl der Scans von einer IP-Adresse aus streng zu limitieren, oder die Zeit zwischen den Scans stark zu variieren, etc.	mittel
• Manuelle Verifikation der übrigen Schwachstellen, wie z. B. Tests von Buffer-Overflow Exploits, etc.	hoch bis sehr hoch
Risiken:	
Systeme können beim Ausnutzen der Schwachstellen abstürzen oder in ihrer ordnungsmäßigen Funktion beeinträchtigt werden. Die Versuche, identifizierte Schwachstellen auszunutzen, können erkannt werden.	

E 2. Offensichtliche Verifikation tatsächlicher Schwachstellen	
Es werden die identifizierten Schwachstellen auf ihr tatsächliches Gefährdungspotenzial hin untersucht, indem versucht wird, die Schwachstelle mit dem Ziel der Kompromittierung des Systems auszunutzen.	
Erwartete Ergebnisse:	**erledigt**
• Ergänzte Liste der Patchlevel von Systemen und Anwendungen	☐
• Liste der tatsächlichen Schwachstellen	☐
• Liste der potenziellen Schwachstellen, die nicht verdeckt verifiziert werden können	☐
Voraussetzungen:	
Ergebnisse I 12: Liste der potenziellen Schwachstellen	
Prüfungsschritte:	**Aufwand**
• Einsatz von aktuellen Schwachstellenscannern (siehe A.7).	mittel
• Manuelle Verifikation der übrigen Schwachstellen, wie z. B. Tests von Buffer-Overflow Exploits, etc.	hoch bis sehr hoch
Risiken:	
Systeme können beim Ausnutzen der Schwachstellen abstürzen oder in ihrer ordnungsmäßigen Funktion beeinträchtigt werden.	

E 3. Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen	
Es werden die identifizierten Schwachstellen in Kommunikationsbeziehungen (Schnittstellen), z. B. bei Datenbankzugriffe durch einen Webserver, auf ihr tatsächliches Gefährdungspotenzial hin untersucht, indem versucht wird, die Schwachstelle mit dem Ziel der Kompromittierung des Systems auszunutzen.	
Erwartete Ergebnisse:	**erledigt**
• Ergänzte Liste der Patchlevel von Systemen und Anwendungen	☐
• Liste der tatsächlichen Schwachstellen in Anwendungsschnittstellen	☐
Voraussetzungen:	
Ergebnisse I 12 und I 13: Detaillierte Systembeschreibungen und Liste der Anwendungsschnittstellen.	
Prüfungsschritte:	**Aufwand**
• Einsatz von aktuellen Schwachstellenscannern (siehe A.7).	mittel
• Manuelle Verifikation der übrigen Schwachstellen, wie z. B. Tests von Buffer-Overflow Exploits, etc.	hoch bis sehr hoch
Risiken:	
Systeme können beim Ausnutzen der Schwachstellen abstürzen oder in ihrer ordnungsmäßigen Funktion beeinträchtigt werden. Die Versuche, identifizierte Schwachstellen auszunutzen, können erkannt werden.	

E 4. Verdeckter Test der Router	
Die identifizierten Router werden auf Schwachstellen und Manipulationsmöglichkeiten hin untersucht.	
Erwartete Ergebnisse:	**erledigt**
• Informationen über Router ACLs	☐
• Informationen über die Routerkonfiguration	☐
• Administrativer Zugriff auf Router	☐
Voraussetzungen:	
Ergebnis I 8: Liste mit Detailinformationen über identifizierte Router	
Prüfungsschritte:	**Aufwand**
• Versuch des Logins auf den Router mit Standardpasswörtern. Von Brute Force Attacken sollte abgesehen werden, da diese leicht zu entdecken sind (z. B. durch ein IDS) und der Test verdeckt stattfinden soll.	mittel
• Ermittlung der Router ACLs mit Hilfe geeigneter Tools (Firewalking). Bei der Durchführung sollte darauf geachtet werden, dass der Test über einen größeren Zeitraum „gesteckt“ wird, um eine Identifikation des Angriffs zu erschweren.	hoch
• Überprüfung der Reaktion des Routers auf fragmentierte und gespoofte Pakete, die mittels eines Paketgenerators erzeugt wurden. Bei der Durchführung sollte darauf geachtet werden, dass der Test über einen größeren Zeitraum „gesteckt“ wird, um eine Identifikation des Angriffs zu erschweren.	sehr hoch
Risiken:	
Der Angriff könnte entdeckt werden. Der überprüfte Router könnte in seiner Funktion beeinträchtigt werden.	

E 5. Offensichtlicher Test der Router	
Die identifizierten Router werden auf Schwachstellen und Manipulationsmöglichkeiten hin untersucht.	
Erwartete Ergebnisse:	**erledigt**
• Informationen über Router ACLs	☐
• Informationen über die Routerkonfiguration	☐
• Administrativer Zugriff auf Router	☐
Voraussetzungen:	
Ergebnis I 9: Liste mit Detailinformationen über identifizierte Router	
Prüfungsschritte:	**Aufwand**
• Versuch des Logins auf den Router mit Standardpasswörtern und Brute-Force Attacken.	mittel
• Ermittlung der Router ACLs mit Hilfe geeigneter Tools (Firewalking)	sehr hoch
• Überprüfung der Reaktion des Routers auf fragmentierte und gespoofte Pakete, die mittels eines Paketgenerators erzeugt wurden.	sehr hoch
Risiken:	
Der überprüfte Router könnte in seiner Funktion beeinträchtigt werden.	

E 6. Test von Vertrauensbeziehungen zwischen Systemen	
Es wird versucht über evtl. vorhandene Vertrauensbeziehungen zwischen Systemen unberechtigten Zugriff zu erhalten, z. B. durch das Ausnutzen von so genannten „trusted Hosts“ bei der Benutzer Authentifizierung.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung über Vertrauensbeziehungen zwischen Systemen	☐
• Unbefugte Informationsgewinnung	☐
• Unbefugter Zugriff auf Dateien oder Systeme	☐
Voraussetzungen:	
Ergebnisse I 6 und I 7: System- und Anwendungsbeschreibungen	
Prüfungsschritte:	**Aufwand**
• Auswertung der bereits vorliegenden Informationen in Bezug auf mögliche Abhängigkeiten und Vertrauensbeziehungen zwischen Systemen.	hoch
• Versuch des Zugriffs mittels Spoofing von IP-Adressen oder anderen Authentifizierungsmerkmalen	sehr hoch
Risiken:	
Die überprüften Systeme könnten in ihrer Funktion beeinträchtigt werden.	

E 7. Verdeckter Test der Firewall von außen	
Es wird versucht, das Firewallsystem zu umgehen, d. h. eine Netzwerkverbindung von außen in das geschützte Netzsegment aufzubauen. Dazu kann z. B. versucht werden, die Kontrolle über das Firewallsystem zu erlangen oder Fehlkonfigurationen auszunutzen.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der von außen ableitbaren Firewallregeln	☐
• Verifikation von identifizierten Schwachstellen der eingesetzten Firewall	☐
• Auflistung der erreichbaren Systeme hinter der Firewall	☐
Voraussetzungen:	
Ergebnisse I 9: Informationen über die eingesetzten Firewallkomponenten	
Prüfungsschritte:	**Aufwand**
• Ermittlung der Firewallregeln mit Hilfe geeigneter Tools (Firewalking)	hoch
• Versuch, Systeme hinter der Firewall zu erreichen	sehr hoch
• Überprüfung der Reaktion der Firewall auf fragmentierte und gespoofte Pakete, die mittels eines Paketgenerators erzeugt wurden.	sehr hoch
Risiken:	
Das Firewallsystem könnte in seiner Funktion beeinträchtigt werden. Der Angriff auf die Firewall könnte z. B. durch die Log-Funktion der Firewall entdeckt werden.	

E 8. Offensichtlicher Test der Firewall von außen	
Es wird versucht, das Firewallsystem zu umgehen, d.h. eine Netzwerkverbindung von außen in das geschützte Netzsegment aufzubauen. Dazu kann z. B. versucht werden, die Kontrolle über das Firewallsystem zu erlangen oder Fehlkonfigurationen auszunutzen.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der von außen ableitbaren Firewallregeln	☐
• Verifikation von identifizierten Schwachstellen der eingesetzten Firewall	☐
• Auflistung der erreichbaren Systeme hinter der Firewall	☐
Voraussetzungen:	
Ergebnisse I 10: Informationen über die eingesetzten Firewallkomponenten	
Prüfungsschritte:	**Aufwand**
• Einsatz eines Schwachstellenscanners auf die Hosts des Firewall-Systems (Firewall-Host, externer Router, interner Router)	mittel
• Ermittlung der Firewallregeln mit Hilfe geeigneter Tools (Firewalking)	hoch
• Versuch, Systeme hinter der Firewall zu erreichen	sehr hoch
• Überprüfung der Reaktion der Firewall auf fragmentierte und gespoofte Pakete, die mittels eines Paketgenerators erzeugt wurden	sehr hoch
Risiken:	
Das Firewallsystem könnte in seiner Funktion beeinträchtigt werden.	

E 9. Beidseitiger Test der Firewall	
Untersuchung der Firewall durch gleichzeitigen Test auf beiden Seiten der Firewall: Ein „außen“ platziertes System sendet Pakete, ein „innen“ platziertes System analysiert die durchkommenden Pakete und umgekehrt.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung der Firewallregeln	☐
• Verifikation von identifizierten Schwachstellen des eingesetzten Firewalltyps	☐
• Vervollständigte Auflistung der erreichbaren Systeme hinter der Firewall	☐
Voraussetzungen:	
Ergebnisse I 10: Informationen über die eingesetzten Firewallkomponenten, Netzzugang zu einem Punkt hinter der Firewall.	
Prüfungsschritte:	**Aufwand**
• Test, ob (u. U. auch mit Hilfe von getunnelten Protokollen) unzulässige Verbindungen aus dem internen Netz ins Internet aufgebaut werden können	hoch
• Einsatz eines Schwachstellenscanners auf die Hosts des Firewall-Systems (Firewall-Host, externer Router, interner Router) von innen	mittel
• Ermittlung der Firewallregeln mit Hilfe geeigneter Tools (beidseitiges Firewalking)	hoch
• Überprüfung der Reaktion der Firewall auf fragmentierte und gespoofte Pakete, die mittels eines Paketgenerators erzeugt wurden	sehr hoch
Risiken:	
Das Firewallsystem könnte in seiner Funktion beeinträchtigt werden.	

E 10. Test des IDS-Systems	
Es wird getestet, ob ein evtl. vorhandenes IDS die potentielle Angriffe registriert und Alarme auslöst.	
Erwartete Ergebnisse:	**erledigt**
• Typ des IDS	☐
• Verhalten des IDS auf verschiedene Angriffstypen	☐
• Aussage zur Performance des IDS	☐
Voraussetzungen:	
Detaillierte System- und Firewallinformationen. Möglichkeit, die Alarmauslösung des IDS-Systems zu überwachen.	
Prüfungsschritte:	**Aufwand**
• Durchführung von schrittweise offensichtlicheren Angriffsarten auf das Netzwerk der Zielorganisation	gering bis sehr hoch
• Evaluation der Reaktion des IDS auf die Angriffe	sehr hoch
• Abgleich der Angriffs- und IDS-Logfiles	hoch
Risiken:	
Durch die Prüfungsschritte kann die Funktionsfähigkeit des Netzes der Zielorganisation beeinträchtigt werden.	

E 11. Abhören von Passwörtern	
Es wird versucht, durch den Einsatz von Abhör-Tools (Netzwerk-Sniffern, Backdoors, etc.) Passworte abzuhören.	
Erwartete Ergebnisse:	**erledigt**
• Passwörter im Klartext	☐
Voraussetzungen:	
Zur Installation von Abhör-Tools sind geeignete Systemrechte erforderlich. Diese können u.a. durch eine vorher identifizierte Schwachstelle erlangt werden. Die datenschutzrechtlichen Voraussetzungen sind zu beachten	
Prüfungsschritte:	**Aufwand**
• Erlangung von Rechten zur Installation von Abhör-Tools auf geeigneten Systemen	sehr hoch
• Installation von Abhör-Tools auf geeigneten Systemen	hoch
• Aufzeichnung und Auswertung des Netzwerkverkehrs auf übertragene Passwörter	hoch
Risiken:	
Durch die notwendige Installation von Abhör-Tools auf geeigneten Systemen können diese Systeme in Ihrer Funktion beeinträchtigt werden. Durch die notwendige Installation von Abhör-Tools auf geeigneten Systemen werden diese Systeme evtl. auch für nicht autorisierte Dritte zugänglich.	

E 12. Test von Passwörtern	
Es wird versucht, durch verschiedene Methoden ein Passwort zu ermitteln, das einen privilegierten Zugang zu einem System / einer Anwendung ermöglicht.	
Erwartete Ergebnisse:	**erledigt**
• Passwörter im Klartext	☐
Voraussetzungen:	
Zur Durchführung von Offline-Attacken müssen Passwort-Files, die die verschlüsselten Passwörter enthalten, vorhanden sein, z. B. aus E 11 oder vom Auftraggeber geliefert. Für Online-Attacken muss ein Verbindungsaufbau zu den geschützten Systemen möglich sein.	
Prüfungsschritte:	**Aufwand**
• Überrüfung der Passwortdateien mittels geeigneter Tools (Offline)	mittel bis sehr hoch
• Durchführung von Online Attacken, wenn kein Passwortfile für eine Offline-Attacke zur Verfügung steht.	hoch
• Manueller Test von Standardpasswörtern oder häufig verwendeten Passwörtern	mittel
Risiken:	
Benutzerkonten könnten gesperrt werden, wenn in der zu testenden Anwendung/Betriebssystem ein Maximalwert für fehlerhafte Passworteingaben definiert wurde.	

E 13. Test von „Denial-of-Service“ Anfälligkeit	
Es wird überprüft, inwieweit das System anfällig für eine Denial-of-Service-Attacke ist.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung von Systemen, die anfällig für DoS-Attacken sind	☐
Voraussetzungen:	
Es müssen für DoS-Attacken anfällige Systeme (Webserver, Mailserver etc.) zur Verfügung stehen.	
Prüfungsschritte:	**Aufwand**
• Auswertung der Ergebnisse aus Modul I 12: Recherche nach Schwachstellen	mittel
• Durchführung einer DoS-Attacke mit verschiedenen Mitteln	mittel bis sehr hoch
Risiken:	
Selbst wenn der Test ergibt, dass das betreffende System nicht anfällig für eine DoS-Attacke ist, kann evtl. durch einen groß angelegten verteilten DoS-Angriff (DDoS: Distributed DoS), der für einen Penetrationstester nur schwer darstellbar wäre, dennoch ein erfolgreicher Angriff durchgeführt werden. Das getestete System oder beteiligte Netzkomponenten können in ihrer Funktionsfähigkeit beeinträchtigt werden oder abstürzen.	

E 14. Computerbasiertes Social-Engineering	
Es wird versucht, auf eine Person Einfluss zu nehmen, um unter Anwendung geeigneter computertechnischer Manipulationstechniken, z. B. durch das Ausnutzen von Neugierde oder Hilfsbereitschaft, Systemrechte zu erhalten.	
Erwartete Ergebnisse:	**erledigt**
• Zugangsmöglichkeiten zum Netz oder Systemen der Organisation	☐
• Auflistung von System- und Anwendungspasswörtern	☐
Voraussetzungen:	
Ergebnisse I 6, I7, I 13 - I 16,: Informationen über Zielsysteme, -anwendungen und –personen.	
Prüfungsschritte:	**Aufwand**
• Kontaktaufnahme mit der Zielperson per E-Mail	mittel
• Zielpersonen täuschen und zur Installation von speziellen Programmen (z. B. Keylogger) veranlassen	mittel bis hoch
• Zielperson durch gefälschte Systemmeldungen zur Eingaben von Benutzernamen und Passwort auffordern	mittel bis hoch
Risiken:	
Der Angriff könnte als solcher bemerkt werden und Irritationen bei der Zielperson auslösen. Die speziellen Programme könnten den Betrieb stören.	

E 15. Direktes, persönliches Social-Engineering mit physischem Zutritt	
Es wird versucht, durch direkte Kontaktaufnahme zu einer Person (z. B. durch Besuch), die über ein privilegiertes Wissen verfügt, an vertrauliche Informationen zu gelangen. Dabei wird z. B. versucht, unter Vortäuschung eines Vertrauensverhältnisses die Zielperson zur Preisgabe von Informationen zu bewegen. Bei der Zielperson kann es sich um Mitarbeiter der Organisation oder andere Insider handeln.	
Erwartete Ergebnisse:	**erledigt**
• Relevanten Informationen wie Passwörter, Systemkonfigurationen etc.	☐
Voraussetzungen:	
Ergebnisse I 7, I 14 - I 16: Informationen über Zielsysteme, -anwendungen und –personen.	
Prüfungsschritte:	**Aufwand**
• Persönliche Kontaktaufnahme mit der Zielperson (z. B. als Service-Techniker, neuer Mitarbeiter, etc.)	mittel
• Vortäuschung eines Vertrauensverhältnisses, um die Zielperson zur Herausgabe von Informationen zu bewegen (z. B. die Herausgabe eines Schlüssels oder Bekanntgabe von Passwörtern)	hoch
Risiken:	
Der Angriff könnte als solcher bemerkt werden und Irritationen bei der Zielperson auslösen. Falls es zur Herausgabe von relevanten Informationen kommt, könnte dieser Umstand, nachdem der Penetrationstest aufgelöst wird und sich die Zielperson ihres Fehlverhaltens bewusst wird, die Beziehung zwischen Zielperson und Zielorganisation belasten, vor allem wenn es sich um einen Mitarbeiter der Zielorganisation handelt	

E 16. Indirektes, persönliches Social-Engineering ohne physischen Zutritt	
Es wird versucht, durch fernmündliche Kontaktaufnahme zu einer Person, die über ein privilegiertes Wissen verfügt, Geheimnisse auszuforschen. Dabei wird z. B. versucht, unter Vortäuschung eines Vertrauensverhältnisses die Zielperson zur Preisgabe von Informationen zu bewegen. Bei der Zielperson kann es sich um Mitarbeiter der Organisation oder andere Insider handeln. Hierbei wird die Naivität der Mitarbeiter der Zielorganisation und deren Bedürfnis involviert und hilfsbereit zu sein ausgenutzt.	
Erwartete Ergebnisse:	**erledigt**
• Relevanten Informationen wie Passwörter, Systemkonfigurationen etc.	☐
Voraussetzungen:	
Ergebnisse I7, I14 - I16: Informationen über Zielsysteme, -anwendungen und –personen.	
Prüfungsschritte:	**Aufwand**
• Kontaktaufnahme mit der Zielperson per Telefon oder E-Mail	mittel
• Vortäuschung eines Vertrauensverhältnisses, um die Zielperson zur Herausgabe von Informationen zu bewegen (z. B. Ausgabe als Administrator, Mitarbeiter, entfernter Vorgesetzter etc.)	hoch
Risiken:	
Der Angriff könnte als solcher bemerkt werden und Irritationen bei der Zielperson auslösen. Falls es zur Herausgabe von relevanten Informationen kommt, könnte dieser Umstand, nachdem der Penetrationstest aufgelöst wird und sich die Zielperson ihres Fehlverhaltens bewusst wird die Beziehung zwischen Zielperson und Zielorganisation belasten. (Vor allem wenn es sich um einen Mitarbeiter der Zielorganisation handelt)	

E 17. Überprüfung der drahtlosen Kommunikation	
Es wird versucht, Zugang zu einem vorhandenen WLAN zu erreichen.	
Erwartete Ergebnisse:	**erledigt**
• Auflistung von Schwachstellen des WLAN	☐
Voraussetzungen:	
Ergebnis I 17: Informationen über ein eventuell installiertes WLAN	
Prüfungsschritte:	**Aufwand**
• Analyse der Ergebnisse des Moduls I 17: Überprüfung der drahtlosen Kommunikation (nur scannend)	mittel
• Ausnutzen von möglichen Schwachstellen	sehr hoch
• Versuch, Verbindung zu einem WLAN aufzubauen	mittel
• Versuch, Zugang zu dem WLAN zu erhalten	hoch
• Versuch, Zugriff auf Daten im WLAN zu erhalten	sehr hoch
Risiken:	
Die Funktionsfähigkeit des WLANs könnte durch den Penetrationstest beeinträchtigt werden.	

E 18. Test der administrativen Zugänge zur Telefonanlage	
Es wird versucht, administrativen Zugang zur Telefonanlage zu erhalten. Insbesondere Fernwartungszugänge, die nicht durch ein statisches Call-Back-Verfahren geschützt sind, oder voreingestellten Standard-Passwörter und –PINs bergen ein hohes Risiko.	
Erwartete Ergebnisse:	**erledigt**
• Administrativer Zugang zur Telefonanlage	☐
Voraussetzungen:	
Ergebnisse I 18: Informationen über die Telefonanlage	
Prüfungsschritte:	**Aufwand**
• Analyse der Ergebnisse des Moduls I 18: Test der Telefonanlage (Identifikation)	hoch
• Versuch, administrativen Zugang zur Telefonanlage zu erhalten	sehr hoch
Risiken:	
Die Funktionsfähigkeit der Telefonanlage könnte durch die Prüfungsschritte beeinträchtigt werden.	

E 19. Test des Voicemailsystems	
Es wird versucht, die Sicherheitsfunktionen des Mailboxsystems zu umgehen und Zugriff auf Mailboxen zu erhalten.	
Erwartete Ergebnisse:	**erledigt**
• Zugriff auf einige Mailboxen	☐
Voraussetzungen:	
Ergebnisse I 19: Informationen über das eingesetzte Voicemailsystem	
Prüfungsschritte:	**Aufwand**
• Analyse der Ergebnisse von Modul I 19: Test des Voicemailsystems (Identifikation)	mittel
• Test, ob Zugriff anhand der voreingestellten Passwörter / Codenummern möglich ist.	mittel
• Durchführung weiterer technischer Tests, die ein spezifisches Wissen über das eingesetzte Modell der Telefonanlage voraussetzen.	sehr hoch
Risiken:	
Betroffene Mailboxinhaber werden evtl. in ihren Grundrechten (Schutz der Privatsphäre) beeinträchtigt.	

E 20. Test der administrativen Zugänge zum Faxsystems	
Es wird versucht, die Sicherheitsfunktionen des Faxsystems zu umgehen und administrativen Zugang zum Faxsystem zu erhalten.	
Erwartete Ergebnisse:	**erledigt**
• Administrativer Zugriff auf Faxsystem	☐
• Verifikation von Schwachstellen	☐
Voraussetzungen:	
Ergebnisse I 20: Informationen über das Faxsystem	
Prüfungsschritte:	**Aufwand**
• Analyse der Ergebnisse aus Modul I 20: Test des Faxsystems (Identifikation)	mittel
• Durchführung weiterer technischer Tests, die ein spezifisches Wissen über das eingesetzte Faxsystem voraussetzen.	sehr hoch
Risiken:	
Die Funktionsfähigkeit des Faxsystems könnte durch die Prüfungsschritte beeinträchtigt werden.	

E 21. Test von Modems	
Es wird versucht, über nicht abgesicherte Modems Zugang zum Netzwerk der Zielorganisation unter Umgehung der Firewall zu erhalten.	
Erwartete Ergebnisse:	**erledigt**
• Liste von „wilden“ Modems	☐
• Liste über gelungene Penetrationsversuche	☐
Voraussetzungen:	
Telefonnummernbereiche oder Liste mit Modem-Telefonnummern	
Prüfungsschritte:	**Aufwand**
• Einsatz eines Wardialers (mit Systemerkennungskomponente) auf den Telefonnummernbereich der Zielorganisation	hoch
• Penetrationsversuch des Netzwerks über die identifizierten Modem-verbindungen	sehr hoch
Risiken:	
Keine	

E 22. Aktiver Test der Zutrittskontrollen	
Es wird versucht, Zutrittskontrollmechanismen zu überwinden um physischen Zutritt zu den Gebäuden und Räumen der Zielorganisation zu erhalten.	
Erwartete Ergebnisse:	**erledigt**
• Erlangung von Zutritt zu geschützten Bereichen	☐
Voraussetzungen:	
Ergebnisse I 22: Informationen über die Zutrittskontrollen	
Prüfungsschritte:	**Aufwand**
• Auswertung der Ergebnisse aus Modul I 22: Identifikation von Zutrittskontrollen	mittel
• Test, ob Zutritt zum Gelände / zum Gebäude der Zielorganisation unter einem Vorwand gewährt wird	mittel
• Test, ob Zutritt unbemerkt zum Gelände / zum Gebäude der Zielorganisation möglich ist	mittel
• Weitergehende Tests, ob Zutritt zu Serversystemen oder Arbeitsplatzrechnern erlangt werden kann	hoch
Risiken:	
Eine Entdeckung des Zutrittsversuchs könnte zu Irritationen bei den Mitarbeitern der Zielorganisation führen und/oder die Alarmierung der Polizei zur Folge haben.	

E 23. Überprüfung der Eskalationsprozeduren	
Es wird überprüft, inwieweit die etablierten Eskalationsprozeduren im Angriffsfall eingehalten werden und wie effektiv und effizient die Prozeduren sind.	
Erwartete Ergebnisse:	**erledigt**
• Beurteilung über Funktionsfähigkeit der etablierten Eskalationsprozeduren in der Praxis	☐
Voraussetzungen:	
Die Möglichkeit, die Reaktionen der Mitarbeiter des Auftragsgeber auf die Angriffsversuche zu überwachen.	
Prüfungsschritte:	**Aufwand**
• Es werden schrittweise offensichtlichere Angriffsarten auf das Netz der Zielorganisation ausgeführt um Eskalationsprozeduren zu aktivieren	gering bis sehr hoch
• Die Aufzeichnungen der durchgeführten Angriffe werden mit den ergriffenen Gegenmaßnahmen abgeglichen. Die Gegenmaßnahmen werden auf ihre Angemessenheit hin beurteilt	mittel
Risiken:	
Durch die Prüfungsschritte kann die Funktionsfähigkeit des Netzes der Zielorganisation beeinträchtigt werden.	

6.6 Dokumentation des Penetrationstests

Der Umfang und Inhalt der Dokumentation, der nach Abschluss der Prüfung an den Auftraggeber übergeben werden soll, muss vertraglich vereinbart werden. Zu einer vollständigen Dokumentation können gehören:

- der Vertrag inklusive der Ergebnisse und Vereinbarungen, die im Vorbereitungsgespräch abgestimmt worden sind (siehe 4.3),
- die Dokumentation der abgearbeiteten Prüfungsschritte zur Informationsbeschaffung, z. B. mittels Vorlage A.6.1, die Logfiles der eingesetzten Tools einschließlich der Liste der geprüften Schwachstellen,
- die daraus abgeleiteten Systembeschreibungen (siehe Vorlage A.6.3),
- die Liste der potenziellen Schwachstellen, aufgeschlüsselt nach System und einschließlich einer Kurzbeschreibung
- die Ergebnisse der Risikoanalyse (Aufwand und Prioritäten) und die damit ausgewählten Systeme bzw. E-Module für Phase 4 (aktive Eindringversuche),
- die Dokumentation der abgearbeiteten Module für aktive Eindringversuche, z. B. mittels Vorlage A.6.2 und die Logfiles der eingesetzten Tools,
- die einzelnen Ergebnisse der E-Module einschließlich der Liste der verifizierten Schwachstellen,
- sowie ein Abschlussbericht.

Falls besonders hohe Ansprüche an die Nachvollziehbarkeit des Penetrationstests gestellt werden, so können weitere Maßnahmen zur Dokumentation notwendig werden. Möglich ist z. B. der Einsatz von Tastatur-, Maus-Recordern und Bildschirm- bzw. Terminal Logging-Utilities und/oder von Netzwerkmonitoren/Sniffern.

Die einzelnen Teile der Dokumentation könne sehr sicherheitssensitive Informationen enthalten, wie z. B. Passwörter oder offene Schwachstellen. Daher muss die gesamte Dokumentation vertraulich behandelt werden. Desweiteren muss vereinbart werden, wer beim Auftraggeber welche Teile der Dokumentation erhält. Bestimmte Teile, z. B. personenbezogene Daten, sollten nur dem Datenschutzbeauftragten übergeben werden und nicht der IT-Abteilung.

7 Durchführung von Penetrationstests

In diesem Kapitel wird anhand von konkreten Beispielen die Durchführung von Penetrationstest nach der vorgestellten Methodik beschrieben. Dazu werden die jeweiligen Schritte in den Phasen 1 – 5 detailliert erläutert und auf mögliche Problemfelder hingewiesen. Desweiteren wird hervorgehoben, welche Dokumentation an welcher Stelle zu erstellen ist.

7.1 Vorbereitung

Abbildung 4: Phase 1 – Vorbereitung des Penetrationstests

Die Vorbereitungsphase beginnt mit der Definition des Ziels bzw. der Ziele des Penetrationstests. Dies sollten Auftraggeber und Auftragnehmer gemeinsam durchführen, damit beide Partner von den gleichen Vorraussetzungen ausgehen. Mögliche Ziele des Penetrationstests sind Erhöhung der Sicherheit der technischen Systeme, Bestätigung der IT-Sicherheit durch einen externen Dritten, sowie die Erhöhung der Sicherheit der organisatorischen / personellen Infrastruktur (vgl. Kap. 3.2).

In Abhängigkeit von den vereinbarten Zielen müssen die rechtlichen Aspekte für die Durchführung des Penetrationstests (vgl. Kap. 4.2) sowie organisatorische, personelle und technische Vorraussetzungen (vgl. Kap. 5.1, 5.2 und 5.3) beachtet und zwischen Auftraggeber und –nehmer diskutiert werden.

Nun wird mit Hilfe der Klassifikation (vgl. Kap. 3.4) anhand der sechs Kriterien Informationsbasis, Aggressivität, Umfang, Vorgehensweise, Technik und Ausgangspunkt der gewünschte Test konkretisiert.

Wird ein Penetrationstest das erste Mal durchgeführt, so sollte der Test möglichst alle vorhandenen Systeme umfassen, da sonst Schwachstellen in nicht berücksichtigten Systemen verbleiben könnten.

Der zeitliche Umfang, der für die Prüfungstätigkeiten aufgewendet werden soll, kann idealerweise durch die Resultate einer zuvor durchgeführten Schutzbedarfsanalyse, z. B. nach der Methode des Grundschutzhandbuchs [BSI02], abgeschätzt werden.

Anhand der getroffenen Klassifizierung wird anschließend über das Ausschlussprinzip bestimmt, welche Module zur Informationsbeschaffung und für aktive Eindringversuche ausgelassen bzw. durchgeführt werden (vgl. 6.4.1).

Je nach Auswahl der Module ergeben sich entweder höhere oder niedrigere Risiken für den Auftraggeber, beispielsweise Verschiebung von durchzuführenden Wartungsarbeiten (niedriges Risiko) oder der permanente Ausfall eines IT-Systems (hohes Risiko). Diese Risiken gilt es zwischen Auftraggeber und Auftragnehmer hinsichtlich Eintrittswahrscheinlichkeit und Wirkung zu diskutieren. Für die Risiken, die beide Vertragspartner gewillt sind zu tragen, sollten als Ergebnis der Diskussion die erforderlichen Notfallmaßnahmen vereinbart werden. Bei der Abstimmung der Notfallmaßnahmen muss insbesondere das Zeitfenster, in dem kritische Tests durchgeführt werden dürfen und die Verantwortung für die erforderlichen Maßnahmen berücksichtigt werden. Falls sich aus der Auswahl der Module inakzeptable Risiken ergeben, so muss ein anderer Penetrationstest ausgewählt werden, z. B. ein weniger aggressives Vorgehen bei den aktiven Eindringversuchen, ein Verzicht auf den Einsatz von Social-Engineering-Techniken oder ein geringerer Umfang der zu testenden Systeme. Gegebenfalls sind nun erneut die organisatorischen und rechtlichen Rahmenbedingungen zu berücksichtigen bzw. zu diskutieren.

Sämtliche Ergebnisse der Vorbereitungsphase sollten in einem Protokoll schriftlich festgehalten und von den beiden Vertragspartner unterschrieben werden. Dieses Protokoll kann dem Auftraggeber beispielsweise als Kontrollinstrument des Penetrationstests und dem Auftragnehmer als Vorgehensrichtlinie dienen.

Darüberhinaus sollte der Umfang der nach der Durchführung des Penetrationstests zu übergebenden Dokumentation vertraglich vereinbart werden. Ziel der Dokumentation sollte sein, dass die Durchführung des Penetrationstests nachvollziehbar wird. Einen Hinweis zu Dokumentationstechniken von Penetrationstests befindet sich in Kapitel 6.6, passende Dokumentationsvorlagen sind im Anhang A.5.1 zu finden.

Ergebnis der Vorbereitungsphase muss ein detaillierter Plan sein, der genau vorgibt wann welche Komponenten mit welcher Intensität penetriert werden. Darüber hinaus müssen Eskalationsstufen vereinbart werden, d. h. für sensitive Systeme müssen Notfallmaßnahmen erarbeitet werden wie Datensicherungen, Ersatzsysteme bzw. welche Dienstleister müssen zur Verfügung stehen.

Die Testzeiträume sollten zumindest für geschäftskritischen Systemen grob definiert werden, um z. B. nicht den operativen Ablauf des Auftraggebers zu stören. Eventuell muss geklärt werden wer aus den Fachabteilungen über den Test informiert werden muss.

Eine Klassifizierung der Daten hilft die Intensität und das Vorgehen für die Tests festzulegen (Produktivserver wird anders getestet als Testserver). Soll z. B. ein Cluster getestet werden, muss geklärt werden, ob an dieser Stelle eine Revision nicht besser geeignet ist, Schwachstellen zu identifizieren. Bei Eigenentwicklungen sollte mit den betreffenden Mitarbeitern aus dem Support festgelegt werden, welche Vorsorgemaßnahmen notwendig und möglich sind.

Letztlich sollte bereits im Vorfeld der Test geklärt werden, wie mit den Ergebnissen aus dem Penetrationstest umgegangen werden soll. Ein positives und konstruktives Vorgehen ist geeignet, um aus den Empfehlungen Maßnahmen zur Verbesserung der IT-Sicherheitsiunfrastruktur abzuleiten und umzusetzen.

7.2 Informationsbeschaffung

Abbildung 5: Phase 2 – Informationsbeschaffung

Die Phase 2: Informationsbeschaffung beginnt mit der Auswertung der Erstinformationen. Im Falle eines Black-Box-Test kann sich die Erstinformation auf eine IP-Adresse bzw. auf einen IP-Adressbereich beschränken. Wurden im Rahmen eines White-Box-Tests umfangreiche Informationen zur Verfügung gestellt (wie beispielsweise Betriebssystemversionen, eingesetzte Applikationen etc.), so sollte der Tester diese zunächst analysieren und falls erforderlich weitere Informationen, wie z. B. Systembeschreibungen, Netzpläne, etc., vom Auftraggeber nachfordern, um einen möglichst effizienten Test zu gewährleisten.

Als nächstes werden nun die Prüfungshandlungen der ausgewählten I-Module durchgeführt. Die Reihenfolge, in der die Module abgearbeitet werden, ist weitestgehend dem Tester überlassen. Nur das Modul I 12: „Recherche nach Schwachstellen“, kann erst nach Abschluss der vorherigen I-Module sinnvoll bearbeitet werden, da es auf deren Ergebnisse angewiesen ist, z. B. die Liste der erreichbaren Systeme und Programmversionen. Die gesammelten Informationen werden in I 12 dazu verwendet, die Verwundbarkeiten der Systeme und Anwendungen zu identifizieren, indem bekannte Schwachstellen und Sicherheitslücken aus öffentlichen und privaten Datenbanken abgefragt werden. Diese Vorgehensweise soll anhand eines Beispiels verdeutlicht werden:

Der Tester hat als ein mögliches Ziel des Penetrationstests einen Server in der DMZ des Auftraggebers als E-Mail-Server identifiziert und hat durch Banner-Lookup die Version der E-Mail-Server-Software und das Betriebssytem des Servers ermittelt. Anhand dieser Informationen sucht der Tester u. a. in Datenbanken, Mailinglisten und Newsgroups nach möglichen Schwachstellen dieser Kombination. Schwachstellen-Scanner können einen Teil dieser Prüfungsschritte automatisieren. Sie stoßen aber bei ungewöhnlichen Kombinationen oftmals an ihre Grenzen und melden nicht bestehende Schwachstellen oder übersehen existierende Schwachstellen. Daher können sie das manuelle Vorgehen nicht ersetzen, allerdings durchaus sinnvoll ergänzen und die Prüfung beschleunigen.

Als Ergebnis der Informationsbeschaffungsphase verfügt der Tester über die ggf. anfallenden Logfiles der I-Module, die z. B. beim Einsatz von Schwachstellenscannern generiert werden, eine Beschreibung der Systeme, sowie über eine Liste der potentiellen Schwachstellen, die allesamt Bestandteil der Dokumentation des Penetrationstests sein sollten.

7.3 Bewertung der Informationen / Risikoanalyse

Abbildung 6: Phase 3 – Bewertung der Informationen und Risikoanalyse

In der ersten Stufe sollte eine Bewertung der Bedrohung stattfinden. Hierbei ist es bei dem meist großen Umfang der erhaltenen Informationen wichtig, die gesammelten Informationen vor dem weiteren Vorgehen zu analysieren und zu bewerten. In diese Bewertung müssen die vereinbarten Ziele, die potentielle Gefährdung der Systeme und der geschätzte Aufwand für die Evaluierung der Sicherheitsmängel einbezogen werden. Eine objektive Bewertung der Schwachstellen und eine Feststellung des Gefährdungspotentials kann beispielsweise anhand des wöchentlich aktualisierten SANS Security Alert Consensus [SANS-SAC] erfolgen. Die Bewertung wird stets einen subjektiven Charakter haben, da z. B. bei der Aufwandsschätzung die Erfahrung und Spezialisierung des Testers einen großen Einfluss hat.

Nachdem die Bedrohung bewertet wurde, sollte der Tester den mit einem erfolgreichen Angriff über die potentiellen Schwachstellen verbundenen individuellen Aufwand abschätzen und ihn mit den Erfolgschancen abwägen. Eine grobe zeitliche Einschätzung für die durchzuführenden Prüfungsschritte kann aus dem angegebenen Aufwand in den Modulbeschreibungen (Aufwand: mittel, hoch, sehr hoch) abgeleitet werden. Aus diesem Vergleich sollte anschließend eine Priorisierung stattfinden: Je höher die Erfolgschancen und je niedriger der Aufwand ist, desto höher sollte die Priorität sein. Sowohl die Aufwandsschätzung als auch die vergebenen Prioritäten sollten vom Tester dokumentiert werden.

Anhand der durch den Tester vorgenommenen Priorisierung können nun die Angriffsziele und Prüfungsschritte für die nachfolgende Phase 4 ausgewählt werden. Die weiteren Prüfungsschritte sollten primär auf die IT-Systeme konzentriert werden, die nach der Bewertung über potentielle Schwachstellen mit hoher bis mittlerer Priorität verfügen bzw. auf die erfolgversprechendsten Prüfungshandlungen beschränkt werden. Dies erfolgt entsprechend durch eine Einschränkung der ausgewählten, durchzuführenden E-Module (vgl. 6.5.2). Eine schriftliche Aufstellung der ausgewähl-

ten Systeme und Module sollte der Dokumentation des Penetrationstests hinzugefügt und vor Durchführung der aktiven Eindringversuche mit dem Auftraggeber abgestimmt werden.

7.4 Aktive Eindringversuche

Abbildung 7: Phase 4 – Aktive Eindringversuche durchführen

Nachdem in den vorherigen Phase die durchzuführenden E-Module ausgewählt und priorisiert wurden, werden die IT-Systeme in dieser Phase aktiv angegriffen. Dabei werden die Angriffsversuche gemäß der zuvor bestimmten Priorität systematisch vom Tester abgearbeitet, beginnend mit der höchsten Priorität.

Da es sich bei der Zielvorgabe eines Penetrationstests durch den Auftraggeber in der Regel um besonders geschäftskritische IT-Systeme handelt, ist bei der Durchführung der Eindringversuche besondere Sorgfalt geboten. Unverzichtbar sind hier die in der Vorbereitungsphase bereits erwähnten Notfallmaßnahmen. Hierunter fallen beispielsweise, dass Durchführen von Eindringversuchen (bei geschäftskritischen Systemen) außerhalb der Arbeitszeiten (also während der Nacht oder am Wochenende) und die Anwesenheit der zuständigen System-Administratoren.

Exemplarisch soll hier anhand des Moduls E 3 „Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen“ die Vorgehensweise illustriert werden:

Es wurde beispielsweise in der Informationsbeschaffungsphase auf einem System ein bestimmtes Server-Betriebssystem mit Webserver-Anwendung identifiziert, das für Online-Transaktionen verwendet wird und das auf das firmeninterne ERP-System zugreift. Die Schwachstellenrecherche ergab, dass es für die dem ERP-System zugrunde liegende Datenbank eine Buffer Overflow-Verwundbarkeit gibt. Der direkte Zugriff auf die Datenbank wird aber durch die eingesetzte Firewall unterbunden. Der Tester steht nun vor der Herausforderung festzustellen, ob z. B. durch eine Manipulation eines HTTP-Links eine geeignete Online-Transaktion ausgelöst werden kann, die durch die Firewall hindurch die Schwachstelle auf dem Datenbanksystem nutzbar macht.

Erst bei den aktiven Eindringversuchen zeigt sich, ob die in der Informationsbeschaffungsphase identifizierten vermeintlichen Schwachstellen auch tatsächlich genutzt werden können, um z. B. in das ausgewählte System einzudringen. Wird vom Auftraggeber gefordert, dass die potenziellen Schwachstellen nicht nur gelistet, sondern auch getestet werden, so sollten Tester und Auftraggeber genau die möglichen Konsequenzen (z. B. Nicht-Verfügbarkeit des Systems) abwägen.

In der Dokumentation sollten sowohl die positiven, d. h. die erfolgreichen aktiven Eindringversuche, als auch die negativen Ergebnisse, d. h. nicht erfolgreiche Eindringversuche, aufgeführt werden.

7.5 Abschlussanalyse / Nacharbeiten / Clean-up

Abbildung 8: Phase 5 – Abschlussanalyse und Nacharbeiten durchführen

In dieser abschließenden Phase werden zuerst die einzelnen Ergebnisse der durchgeführten E-Module gesammelt und in einen Abschlussbericht übertragen. Der Abschlussbericht sollte aus einer Managementzusammenfassung bestehen, die eine Beschreibung des Prüfungsauftrags, der wesentlichen Prüfungsergebnisse und der empfohlenen weiteren Vorgehensweise auf einem abstrakten Niveau beinhaltet und insbesondere für das Top-Management bestimmt ist. Der Hauptteil des Abschlussberichtes sollte je nach Vereinbarung aus den detaillierten positiven und negativen Prüfungsfeststellungen bestehen. Für die Schwachstellen erfolgt eine Bewertung und Priorisierung der Ergebnisse und eine Darstellung der sich daraus ergebenen Risiken durch den Prüfer, damit der Auftraggeber die für die Verfolgung seines Geschäftsbetriebs relevanten Risiken kennt. Zusätzlich sollte der Bericht Empfehlungen beinhalten, wie der Auftraggeber die zum Zeitpunkt des Penetrationstests bestehenden Schwachstellen beseitigen kann. Anhand der Priorisierung der Ergebnisse sollte als Teil des Abschlussberichts zusammen mit dem Auftraggeber ein Aktionsplan für die Behebung der Schwachstellen erstellt werden. Der Aktionsplan sollte für jede kritische Schwachstelle einen Zeitplan und eine für die Behebung verantwortliche Person bzw. einen verantwortlichen Bereich enthalten.

Die während des Penetrationstests gesicherten personenbezognen sensitiven Daten (vgl. 6.6 Dokumentation des Penetrationstests), wie beispielsweise Passwörter oder private E-Mails, sollten aus datenschutzrechtlichen Gründen nicht Bestandteil des Abschlussberichts sein und nach Abschluss nur einer vorher vereinbarten Person, z. B. dem Datenschutzbeauftragten, übergeben werden. Die Arbeitsergebnisse müssen aber für den Auftraggeber eindeutig nachvollziehbar sein, daher sollten alle Informationen aus den einzelnen Phasen zumindest als Anhang in den Arbeitspapieren enthalten sein. Dazu gehören beispielsweise detaillierte Informationen zu den eingesetzten Tools, Arbeitsschrittinfos (welches Tool wurde mit welchen Optionen verwendet), logfiles, Einsatzzeiten (zu welchen Zeiten wurde Angriffe durchgeführt) etc.

Wurden im Rahmen des Penetrationstests Software, wie beispielsweise Keylogger, auf den IT-Systemen des Auftraggebers installiert oder wurden andere Veränderungen an IT-Systemen des Mandanten

vorgenommen, so müssen diese durch den Tester wieder entfernt werden und der gleiche Systemstatus hergestellt werden, wie ihn der Tester vor dem Test vorgefunden hat.

Glossar

Begriff	*Erläuterung*
Back-Door	Computerprogramm, dass einen nicht dokumentierten bzw. geheimen Zugang zum Rechner („Hintertür“) über das Netz einrichtet.
Black-Box-Test	Penetrationstest, bei dem der Tester keine Information im voraus über das zu testende Netz erhält.
Browser	Programm zur Darstellung von Webseiten im Internet / Intranet.
CERT	Computer Emergency Response Team, Gruppe von IT-Spezialisten, die sich mit der Abwehr von Angriffen auf IT-Systeme beschäftigt.
CGI	Common Gateway Interface; Programm zur Verarbeitung von Daten auf einem Webserver, die zuvor von einem ➔ Browser übermittelt wurden.
Cracker	Person, die sich unberechtigterweise und oft mit illegalen Absichten Zugang zu fremden IT-Systemen verschafft oder fremde IT-Systeme manipuliert.
DDoS	Distributed ➔ Denial-of-Service; DoS Angriff, bei dem über viele verteilte Systemen gleichzeitig das Zielsystem angegriffen wird.
Denial-of-Service (DoS)	Angriffstechnik eines Crackers, bei der versucht wird, die Verfügbarkeit eines IT Systems durch Überlastung zu beeinträchtigen.
DMZ	De-Militarized Zone; ein entkoppeltes, isoliertes Teilnetzwerk, das logisch zwischen einem unsicheren und einem zu schützenden Netz platziert ist und meist die von außen erreichbaren Server bzw. Dienste wie Web- und E-Mail-Server enthält.
DNS	➔ Domain Name System
Domain Name System	Mechanismus, mit dem Rechnernamen zu ➔ IP-Adressen aufgelöst werden.
DoS	➔ Denial-of-Service
Eskalationsprozeduren	Handlungsanweisungen, die festlegen, wie im Falle eines erkannten Hacker-Angriffs zu verfahren ist.
Filterregeln	Steuerungsinformationen für eine ➔ Firewall.

Begriff	*Erläuterung*
Firewall	Schutzmaßnahme zwischen zwei Computernetzen, von denen eines einen höheren Schutzbedarf aufweist.
FTP	File Transfer Protocol, Protokoll der Anwendungsschicht zur Übertragung von Dateien.
GoBS	Grundsätze ordnungsgemäßer Buchführungssysteme; aus dem Handelsgesetz abgeleitete Mindestanforderungen an die Funktionalität und Kontrolle von Daten verarbeitenden Systemen.
Hacker	Person, die aus technischem Interesse sich detailliert mit der Funktionalität von Hard- und Software auseinander setzt und dadurch das notwendige Know-How besitzt, Sicherheitsvorkehrungen in Hard- oder Software zu umgehen. Oft wird im allgemeinen Sprachgebrauch nicht zwischen Hackern und ➔ Crackern differenziert, obwohl sich in Fachkreisen diese Unterscheidung durchgesetzt hat.
Hoster	Betreiber eines Serverdienstes.
HTTP	Hypertext Transfer Protocol, Protokoll der Anwendungsschicht zur Darstellung von Webseiten.
IDS	➔ Intrusion Detection System
IKS	➔ Internes Kontrollsystem
Internes Kontrollsystem	Gesamtheit aller Maßnahmen, die einer Organisation dazu dienen, Risiken zu minimieren, Schaden abzuwenden und Vermögen zu sichern.
Internet Service Provider	➔ Provider
Intrusion Detection System	Sicherheits-Software, mit der netzwerkbasierte Angriffe entdeckt und ggf. bekämpft werden können.
IP-Adresse	Nummer, die aus 4 Zahlenblöcken zwischen 0 und 255 (in dezimaler schreibweise) besteht und anhand derer ein System im Internet / Intranet adressiert werden kann.
ISP	➔ Internet Service Provider
LAN	Local Area Network; lokales Netzwerk.
Linux	freies (➔ Open Source) Unix-kompatibles Betriebssystem.
Newsgroups	Nachrichten- bzw. Diskussionsforum im Internet.

Begriff	*Erläuterung*
Open Source	Initiative, die die freie Verfügbarkeit von Software und die Offenlegung des zugehörigen Quellcodes fördert.
OSI-Referenzmodell	7-schichtiges Modell zur Veranschaulichung und zur Standardisierung der Kommunikation zwischen Rechnersystemen.
Outsourcing	Bezug von (bisher selbst erbrachten) Dienstleistungen von Dritten.
P2P-Client	Peer-To-Peer Client: Computerprogramm zum Tausch bzw. zum Herunterladen von Dateien aller Art
Paketfilter	Schutzmechanismus (Firewallfunktionalität), der von einem Router oder einer Firewall auf den Ebenen 1 bis 3 des ➔OSI-Referenzmodells erbracht wird.
Provider	Anbieter eines Dienstes, meist Zugangsvermittlung zum Internet. Auch ein ➔Hoster ist in diesem Sinne ein Provider.
Router	Netzwerkgerät, das zwei oder mehr Netze miteinander verbindet.
Schwachstellen-Scanner	Sicherheits-Software, mit der sich Systeme auf evtl. vorhandenen Software-Schwachstellen und Sicherheitslücken überprüfen lassen.
Security Policy	dt: ➔ Sicherheitsleitlinie
Sicherheitsleitlinie	Dokument, das auf einem hohen Abstraktionsniveau die IT-Sicherheitsziele einer Organisation beschreibt.
SMTP	Simple Mail Transfer Protocol, Protokoll der Anwendungsschicht das hauptsächlich zur Übertragung von E-Mail Nachrichten eingesetzt wird.
Sniffer	Tool, mit dessen Hilfe Netzwerkverkehr abgehört werden kann.
Social-Engineering	Angriffstechnik, bei der versucht wird, durch Täuschung Personen zur Herausgabe von sensiblen Informationen (z. B. Passwörtern) zu bewegen oder in anderer Weise zu manipulieren.
Spoofing	Angriffstechnik eines Crackers, der versucht, durch technische Manipulationen Systeme oder Personen zu täuschen (z. B. Vortäuschung einer falschen IP-Adresse, Vortäuschung einer falschen DNS-Adresse etc.).
TCP/IP	Netzwerkprotokoll, das sowohl im Internet als auch in internen Netzen eingesetzt wird.
Tiger Team	Gruppe von Penetrationstestern.

Begriff	***Erläuterung***
Trojaner	➔ Trojanisches Pferd
Trojanisches Pferd	Programm, das vom Benutzer unbemerkt im Hintergrund schädliche Funktionen ausführt (z. B. Abfangen und Übertragen von Passwörtern)
Vulnerability-Scanner	dt: ➔ Schwachstellen-Scanner
WAN	Wide Area Network; organisationsweites, mehrere Standorte überspannendes Netzwerk.
Wardialer	Hacker-Tool, mit dessen Hilfe sich automatisiert Blöcke von Telefonnummern anwählen lassen und das Informationen über das antwortende Gerät liefert. Wird häufig zum Aufspüren von ungesicherten Modems verwendet.
War Walking	Vorhandensein und Ausdehnung von WLan-Netzwerken ermitteln
War Driving	➔ War Walking mittels KFZ
Web Bug	Unsichtbares Element auf einer Webseite, anhand dessen ein für den Benutzer nicht erkennbares System in der Lage ist, Informationen über die Systemkonfiguration des Benutzers (IP-Adresse, Browser-Version etc.) abzufragen.
Webserver	Rechner, der im Internet abrufbare Informationen bereitstellt.
Webhosting	Betrieb eines ➔Webservers im Auftrag eines Kunden.
White-Box-Test	Penetrationstest, bei dem der Tester vorab Informationen über das zu testende Netz erhält.
WLAN	Wireless Local Area Network; lokales Funknetzwerk.

Literaturverzeichnis

[Andersen99]	Arthur Andersen, KontraG – Erläuterungen zu den wichtigsten Vorschriften und praktische Hinweise zur Umsetzung, 3. Auflage 1999
[Anonymous01]	Anonymous: Der neue Hacker´s Guide, 2. Aufl., Markt & Technik 2001
[BSI02]	Das IT-Grundschutzhandbuch, Stand Mai 2002, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/gshb/index.htm
[BSI01]	Die BSI Firewallstudie II, 2001, http://www.bsi.de/literat/studien/firewall/fwstud.htm
[CCC02]	Chaos Computer Club, http://www.ccc.de/congress/2001/overview.de.html
[CSEG02]	CSEG Communications-Electronic Security Group, http://www.cseg.gov.uk/partnerships/pwi/check/index.htm
[CSI02]	CSI Computer Security Institute, 2002 CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com
[Discovery02]	Discovery.com, http://www.discovery.com/area/technology/hackers/crunch.html
[Emmert02]	Emmert, Ulrich: Strafbare Sicherheits-Tools?, in KES Zeitschrift für Kommunikations- und EDV-Sicherheit, Heft Nr.2, 18. Jhg. 2002, S.6-9
[Fuhrberg01]	Fuhrberg/Häger/Wolf: Internet-Sicherheit, 3. Aufl., Hanser 2001
[GIAC02]	GIAC, 2002, http://www.giac.org
[Herzog02]	Herzog, Pete: Open Source Security Testing Manual OSSTMM, 2002, http://www.isecom.org
[ISACA02]	Information Systems Audit and Control Association, 2002, http://www.isaca.org
[ISACA_CH99]	ISACA Switzerland: Sicherheitsüberprüfung von IT-Systemen mit Hilfe von Tiger Teams, 1999, http://www.isaca.ch
[ISC02]	International Information Systems Security Certifications Consortium, 2002, http://isc2.org
[Kabay00]	Kabay, Michel E.: Social engineering simulations, Network World Security Newsletter, 18.12.2000, http://www.nwfusion.com/newsletters/sec/2000/00292157.html

[Klevinsky02]	Klevinsky/Laliberte/Gupta: Hack I.T. – a guide to security through penetration testing, 1.Aufl., Addison Wesley 2002
[Kurtz02]	Kurtz/McClure/Scambray: Das Anti-Hacker Buch, 3.Aufl., MITP 2002
[LfDN99]	Landesbeauftragter für den Datenschutz Niedersachsen, Grundschutz durch Firewalls, 1999, http://www.lfd.niedersachsen.de
[LfV98]	Landesamt für Verfassungsschutz Baden-Württemberg: Wirtschaftsspionage – die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 1998
[NIST02]	NIST Guideline on Network Security Testing, http://csrc.nist.gov
[SANS]	SANS Institute, http://www.sans.org
[SANS-SAC]	SANS Security Alert Consensus http://www.sans.org/newlook/digests/SAC.htm
[Schneier01]	Schneier, Bruce: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt, 1. Aufl., Wiley 2001
[Sptimes01]	St. Petersburg Times: A history of hacking, http://www.sptimes.com/hackers/history.hacking.html, 2001
[TLC02]	TLC, http://tlc.discovery.com/convergence/hackers/articles/history_03_print.html
[Venema95]	Venema, Wietse: SATAN Security Administrator Tool for Analyzing Networks, http://www.fish.com/satan/
[Vosseberg01]	Vosseberg, Thomas: Hackerz Book, 1.Aufl., Franzis 2001

Anhang

A.1 OSSTMM

Einen relativ großen Bekanntheitsgrad im Bereich der Vorgehensweisen für Penetrationstests hat das Open Source Security Methodology Manual (OSSTMM) [Herzog02]. Das OSSTMM geht auf eine Initiative von Pete Herzog zurück. Dieses Werk ist ein Open Source Projekt, das einen Katalog von Handlungen, die im Rahmen eines Penetrationstests durchgeführt werden müssen, beinhaltet. Diese Vorgehensweise wird von mehreren Autoren ständig weiterentwickelt und der Öffentlichkeit zur Verfügung gestellt. Der zum Zeitpunkt der Erstellung dieser Studie aktuelle Releasestand des OSSTMMs ist Version 2.0 RC 6. Die Zielsetzung des OSSTMMs ist es, einen Qualitätsstandard für die Durchführung von Penetrationstests zu setzen. Adressaten des OSSTMMs sind IT-Security Dienstleister, die auf Ihrem Prüfungsbericht, sofern sie bei der Durchführung des Penetrationstests OSSTMM-konform vorgegangen sind, das OSSTMM-Logo verwenden dürfen.

Das OSSTMM unterteilt den Untersuchungsbereich eines Penetrationstests in die sechs Sektionen („sections“) Internet Security, Information Security, Physical Security, Communications Security, Wireless Security und Social-Engineering. Zu jeder Sektion existieren entsprechende Module („modules“), in denen die zugehörigen Prüfungsbereiche behandelt werden. Diese Module werden jeweils kurz erklärt und die erwarteten Ergebnisse aus der Abarbeitung des Moduls aufgeführt. Die Module bestehen aus Arbeitspaketen („tasks“) mit denen die einzelnen Prüfungsschritte abgehandelt werden. Desweiteren beinhaltet das OSSTMM mehrere Muster zur Dokumentation der Ergebnisse der Prüfungsschritte aus den Einzelmodulen.

Bei der Anwendung des OSSTMM gibt es grundsätzlich 2 Ansätze: Eine sukzessive Abarbeitung der Module hintereinander oder alternativ eine Abarbeitung der Module, bei der unabhängige Module parallel abgearbeitet werden.

Das OSSTMM schlägt zur Messbarmachung, in welcher Regelmäßigkeit die jeweiligen Module wiederholt angewandt werden sollen, eine Metrik, sog. RAVs (Risk Assessment Values), vor. Zu jedem Modul existiert ein Wertepaar, bestehend aus dem „RAV cycle“ und dem „RAV degradation“. Der RAV cycle Wert beschreibt den Zyklus (in Tagen), in dem der Test wiederholt werden sollte. Der RAV degradation Wert gibt an, um wie viel Prozent sich der Sicherheitszustand innerhalb dieses Zyklusses verschlechtert, unter der Annahme, dass der ursprüngliche Test von einem erfahrenen Prüfer unter Berücksichtigung aller Sorgfaltspflichten durchgeführt wurde. In die Berechnung fließt nur der Quotient des Wertepaares ein, d. h. die beiden Werte beeinflussen sich gegenseitig und könnten durch einen einzigen Wert ersetzt werden.

Bei dieser Metrik ist zu beachten, das sie erst mit der neuesten Version (Version 2.0) des OSSTMM eingeführt wurde und deshalb wohl noch einigen Änderungen durch den Open Source Prozess unterworfen sein wird. Darüberhinaus treffen die RAVs keinerlei Aussage über eine absolute Sicherheit, sondern beschreiben lediglich eine zeitliche Abnahme der Sicherheit relativ zum Ausgangswert direkt nach der Durchführung der Prüfung.

In dem OSSTMM Modell wird nicht darauf eingegangen, welches Ziel mit der Durchführung des Penetrationstests verfolgt wird. Es handelt sich um eine Art generisches Arbeitsprogramm, das jedoch individuell angepasst werden kann.

Es findet keine Priorisierung von Modulen bzw. Prüfungshandlungen im Sinne einer „Rangliste“ statt. So werden Tests, mit denen sich weit verbreitete Schwachstellen erkennen lassen, nicht mit höherer Priorität durchgeführt als andere Prüfungshandlungen, die evtl. nur sehr geringe Erfolgswahrscheinlichkeiten in Bezug auf die Kompromittierung eines Systems haben.

A.2 NIST Guideline on Network Security Testing

Ein weiteres erwähnenswertes Modell für die Durchführung von Penetrationstests ist das „Guideline on Network Security Testing“ des National Institute of Standards and Technology (NIST) [NIST02]. Das Dokument befindet sich zum Zeitpunkt dieser Studie noch in Draft-Status.

Inhaltlich gibt die Guideline eine Vorgehensweise zur Überprüfung der Netzwerksicherheit vor und wendet sich an Organisationen, die Ihre eigene IT-Infrastruktur im Rahmen eines Self-Assessment untersuchen möchten. Dabei wird der Bereich „Network Security Testing“ in einen „System´s Life Cycle“ eingeordnet. Darüber hinaus werden ausgewählte Methoden zur Überprüfung der Netzwerksicherheit dargestellt. Dabei wird jedoch nicht die Gesamtheit der beschriebenen Methoden als „Penetration Testing“ bezeichnet, sondern „Penetration Testing“ wird als eine Technik unter mehreren anderen (beispielsweise „Network Mapping“ oder „Password Cracking“) eingeordnet. Die Methode „Penetration Testing“ wird in die sukzessiven Ablaufphasen Planung (Planning), Entdeckung (Discovery), Attacke (Attack) und die parallele Phase Berichterstattung (Reporting) aufgespalten.

A.3 ISACA Switzerland – Sicherheitsüberprüfung von IT-Systemen mit Hilfe von Tiger Teams

Von der Fachgruppe Security der Schweizerischen Informatikgesellschaft und dem ISACA (Information Systems Audit and Control Association) Switzerland Chapter wurde 1999 eine Broschüre mit dem Titel “Sicherheitsüberprüfung von IT-Systemen mit Hilfe von Tiger Teams” veröffentlicht [ISACA_CH99]. Unter dem Begriff “Tiger Team” ist eine Gruppe von Penetrationstestern zu verstehen. Inhaltlich beschäftigt sich die Broschüre mit der Durchführung von Penetrationstests, wobei das Thema in vier Phasen untergliedert wird:

- Akquisition, Offerte und Vertrag
- Risikoanalyse
- Durchführung
- Bericht und Präsentation

Bei dem Werk handelt es sich nicht um ein durchgängiges Vorgehensmodell, vielmehr wurden die einzelnen Kapitel von Sub-Arbeitsgruppen erarbeitet.

Das Kapitel „Akquisition, Offerte und Vertrag“ enthält eine ausführliche Beschreibungen wichtiger Sachverhalte, die im Vorfeld des Penetrationstests einer vertraglichen Regelung bedürfen.

Der Abschnitt „Risikoanalyse“ enthält eine Methodik zur Erfassung und Beurteilung von Gefahren, die mit dem Penetrationstest verbunden sind.

Das Kapitel „Durchführung“ beinhaltet die Arbeitspakete, die innerhalb eines Penetrationstests bearbeitet werden müssen. Im Einzelnen werden folgende Arbeitspakete unterschieden:

1. **Carrier Scan:** Suche nach von außen erreichbaren Modems.
2. **Internet Scan:** Suche nach über das Internet erreichbarer Rechnersysteme und anschließende Identifikation.
3. **Password Cracking:** Überprüfung von Passwörtern bzw. Passwortrichtlinien.
4. **Manuelles Hacking:** Der Versuch, die in 1. –3. identifizierten potentiellen Schwachstellen auszunutzen.
5. **Intranet Scan:** Analog zu 2., nur ausgehend von internen Netz.
6. **System Scan:** Systemanalyse hinsichtlich allgemeiner Konfiguration und überflüssiger Dienste.
7. **Phreaking:** Systeme überprüfen, die mit dem Telefonsystem in Verbindung stehen.
8. **Analyse von Vertrauensbeziehungen:** Beziehungen bzw. Vertrauen zu Geschäftspartnern, Kunden und Lieferanten analysieren.

Im Kapitel „Reporting“ werden die Elemente einer aussagekräftigen Dokumentation und Ergebnisdarstellung erläutert.

Insbesondere das Kapitel „Risikoanalyse“ enthält eine interessante Methode zur Priorisierung und Auswahl von Prüfungshandlungen, die im Rahmen des Penetrationstests durchgeführt werden sollen. Es wird in zwei Schritten eine „Gesamtgefahr“ ermittelt, die als Entscheidungsgrundlage bezüglich des Einsatzes einer bestimmten Technik dient. Diese Teilschritte bestehen aus:

- Gefahrenanalyse des Systems

  Hier wird die Verletzbarkeit des betroffenen Systems durch Hacking-Angriffe bewertet. Dafür werden die Kriterien „Bedrohungsgrad“ (Wie hoch ist der potentielle Bedrohung für das System?), „Hackervoraussetzung“ (Wie begabt muss ein Hacker sein, um die Gefährdung auszunutzen?) und „intern / extern“ (Ist die Bedrohung von innen und / oder außen relevant?) herangezogen.

- Gefahrenanalyse Hacking-Einsatz

  Hier wird der Aufwand und die Erfolgswahrscheinlichkeit einer geeigneten Angriffsmethode beurteilt und um eine Risikobeurteilung der Auswirkung der Attacke ergänzt. Als Ergebnis wird die definitive Entscheidung für oder gegen den Einsatz der Technik getroffen. Als Kriterien stehen „Erfolgschance“ (Wie wahrscheinlich ist der Erfolg der Attacke?), „Aufwand“ (Wie aufwändig ist die Durchführung der Angriffsmethode für den Penetrationstester?) und „Risikobeurteilung“ (Wie gravierend sind die möglichen Auswirkungen der Attacke auf das System?) zur Verfügung.

Anzumerken ist bei der Betrachtung des Werkes als Ganzem, dass Aspekte wie Risikoanalyse und Zielbezogenheit des Penetrationstests aufgegriffen werden. Darüber hinaus enthalten die Kapitel „Vertragsgestaltung“ und „Reporting“ recht detaillierte Ausführungen bezüglich des notwendigen Inhalts von Verträgen und Dokumentationen.

Im Kapitel „Durchführung“ werden Hacker-Techniken beschrieben. Die Zielbezogenheit wird am Anfang des Kapitels aufgegriffen, jedoch nicht in Form eines Auswahlschemas für einzelne Arbeitspakete weiterverfolgt.

A.4 Zertifikationen im Bereich Penetrationstests

A.4.1 Das CHECK Zertifikat der CSEG

Die CSEG (Communications-Electronics Security Group) ist eine Behörde der britischen Regierung, die sich mit Aspekten der IT-Sicherheit auseinander setzt und dabei weitere Behörden in Fragen der IT-Sicherheit berät. Die CSEG hat zur Etablierung eines Standards für IT-Security Dienstleister eine Zertifizierung namens CHECK (Computer IT Health Check Service) eingeführt. Durch die CHECK-Initiative soll Behörden und Unternehmen die Möglichkeit gegeben werden, qualifizierte Anbieter von IT-Sicherheitsprüfung (IT Health Check) anhand des CHECK-„Gütesiegels“ zu identifizieren [CSEG02].

Das Erlangen der CHECK-Zertifizierung ist an eine Mitgliedschaft des IT-Security Dienstleisters im CHECK-Service des CESG gebunden. Diese Mitgliedschaft ist kostenpflichtig, wobei ein jährlicher Beitrag i.H.v. derzeit 7000 engl. Pfund anfällt. Die Mitgliedschaft beinhaltet einen Platz für einen

Teilnehmer bei dem eintägigen „CHECK Service Assault Course“, in dem Hacker-Techniken geschult werden und der mit einer Prüfung abschließt. Bei Bestehen der Prüfung ist der Teilnehmer und die Firma berechtigt, IT-Healthchecks unter Berufung auf das CHECK Schema durchzuführen. Das CHECK-Gütesiegel ist Vorraussetzung zur Durchführung von Aufträgen im nationalen Öffentlichen Bereich und hat Werbewirkung im privaten Wirtschaftssektor.

Voraussetzung für die Aufnahme in das CHECK Service Programm sind die Offenlegung von folgenden Informationen gegenüber dem CESG:

- Einzelheiten zur Geschäftsstruktur des IT-Security Dienstleisters
- Details zur methodischen Vorgehensweise bei Dienstleistungen
- Die Anzahl der in den letzten 12 Monaten durchgeführten Projekte
- eine (anonymisierte) Kopie eines Berichtes über ein IT-Health-Check-Projekt, aus dem Auftragsgegenstand, Prüfungsfeststellungen und Ergebnisse hervorgehen
- Angabe von Ansprechpartnern für Referenzzwecke
- Angaben über evtl. vorhandene weitere Zertifizierungen (ISO 9000)
- Einzelheiten zu den Mitarbeitern: Name, Geburtsdatum, Nationalität und Lebenslauf aller mit der Durchführung von IT-Healthchecks betrauten Mitarbeiter

Das CHECK-Zertifikat erfährt bislang eine moderate Anerkennung in der britischen Wirtschaft. Ein Kritikpunkt ist, dass nur ein einziger Mitarbeiter eines IT-Security Dienstleisters die Prüfung bestehen muss, um damit seiner Organisation den Status eines CHECK-zertifizierten IT-Dienstleisters zu geben.

A.4.2 Das CISSP Zertifikat des ISC²

Von dem International Information Systems Security Certification Consortium (ISC²) wird das CISSP (Certified Internet Security Systems Professional) Zertifikat herausgegeben [ISC02]. Dabei handelt es sich um ein Examen, dessen bestehen zum Tragen des CISSP-Titels berechtigt.

Das ISC² wurde 1988 von einer Gruppe von IT-Security Dienstleistern gegründet. Das Hauptziel der ISC² ist die Schaffung von Standards im Bereich IT-Security. Diese Standards werden als CBKs (Common Body of Knowledge) bezeichnet und stellen eine Sammlung von Informationen zum Thema IT-Security dar.

Ziel der CISSP Initiative ist die Schaffung Zertifikates, mit dem IT-Security Berater ihre Kompetenz nachweisen können. Das CISSP-Programm existiert seit 1992.

Das Examen deckt dabei folgende Themengebiete ab:

- Zugriffsschutzmechanismen und Methoden
- Anwendungs- und Systementwicklung
- Notfallplanung
- Kryptographie
- Rechtliche Grundlagen, forensische Methoden & Ethik
- Sicherheit im laufenden Betrieb
- Physische Sicherheit
- Sicherheitsarchitekturen & Modelle
- Sicherheitsmanagement
- Telekommunikations-, Netzwerk- und Internet-Sicherheit

Das Erlangen des Zertifikates ist neben dem Bestehen des Examens an weitere Bedingungen geknüpft. So muss z. B. der CISSP-Anwärter drei Jahre relevante Berufserfahrung im IT-Security-Bereich und eine Referenz eines bereits zertifizierten CISSP oder seines Arbeitsgebers vorlegen. Darüber hinaus müssen der Ethische Codex der ISC² befolgt und regelmäßig Gebühren an die ISC² entrichtet werden.

In Deutschland ist das CISSP Examen relativ unbekannt. Dies resultiert wohl daher, dass die ISC² bisher in Deutschland nicht vertreten ist. In den USA erfährt das CISSP-Zertifikat eine breite Anerkennung. Genaue Zahlen über bisher zertifizierte CISSPs liegen nicht vor bzw. wurden vom ISC² bisher nicht veröffentlicht.

Seit kurzer Zeit wird vom ISC² auch das SSCP (System Security Certified Practitioner) Examen herausgegeben. Dieses Zertifikat grenzt sich gegenüber dem CISSP in der Weise ab, dass es sich an die Zielgruppe der Netzwerkadministratoren wendet, während das CISSP-Zertifikat die Zielgruppe der Security Berater / Sicherheitsbeauftragte adressiert. Die Inhalte des SSCP-Examens beziehen sich auf folgende Themengebiete:

- Zugriffsschutzmechanismen
- Administration
- Überwachung
- Risiko, Eskalationsprozeduren und Wiederanlaufverfahren
- Kryptographie

- Datenkommunikation
- bösartiger Programmcode / Malware

Über die Verbreitung bzw. Anerkennung, die das SSCP-Zertifikat in der Praxis erfährt, kann derzeit noch keine Aussage gemacht werden.

A.4.3 Das GIAC Zertifikat des SANS Institute

Das SANS (System Administration, Networking and Security) Institute ist eine renommierte Organisation, die sich insbesondere im Themenbereich IT-Security durch verschiedene Veröffentlichungen auszeichnet. Beispielsweise veröffentlicht das 1989 gegründete SANS Institute jährlich die „SANS Top Twenty“, eine Auflistung der 20 verbreitetsten Schwachstellen bei IT-Systemen. [SANS]

Seit 1999 existiert die GIAC-Zertifizierung (Global Information Assurance Certification) mit dem Ziel, IT-Security Beratern die Möglichkeit zu geben, ihren Wissenstand anhand dieses Zertifikates nachzuweisen [GIAC02].

Das GIAC Programm besteht aus mehreren Einzelexamen und unterscheidet sich nach Angaben des SANS Institute von anderen Zertifizierungen, indem es nicht nur theoretisches Wissen abprüft, sondern auch die praktische Umsetzung einbezieht. Darüber hinaus erstrecken sich die GIAC Prüfungen teilweise auch über fortgeschrittene technische Bereiche.

Zertifizierungsziel ist die Erlangung des GSE-Status (GIAC Security Engineer), zu dessen Erreichung das Bestehen von sechs Einzelprüfungen notwendig ist. Darüber hinaus muss der GSE-Anwärter einen Aufsatz über ein Thema mit Bezug zu IT-Security ausarbeiten, der dann auf der Homepage des SANS Institute veröffentlicht wird.

Über die zum GSE benötigten Einzelexamen hinaus existieren noch weitere GIAC Examen für andere Teilgebiete der IT-Security. Die GSE-Einzelexamen sind folgende:

- GSEC (GIAC Security Essentials)
- GCFW (GIAC Certified Firewall Analyst)
- GCIA (GIAC Certified Intrusion Analyst)
- GCIH (GIAC Certified Incident Handler)
- GCNT (GIAC Certified Windows Security Administrator)
- GCUX (GIAC Certified Unix Security Administrator)

Nach Angaben auf der GIAC Homepage waren zum Zeitpunkt der Erstellung dieser Studie 3600 Personen nach GIAC zertifiziert.

A.4.4 Das CISA Zertifikat der ISACA

Die Information Systems Audit and Control Association (ISACA) ist der weltweite Berufsverband der EDV-Prüfer und gibt das CISA (Certified Information Systems Auditor) Zertifikat heraus [ISACA02]. Die ISACA wurde 1968 gegründet und verfügt mittlerweile über 17.000 Mitglieder in 101 Ländern.

Ziel des CISA-Programms ist die Schaffung eines Qualitätsstandards für IT-Prüfer. Das CISA-Programm besteht seit 1978. Die Erlangung des CISA-Titels ist an das Bestehen des CISA Examens, mehrjährige relevante Berufserfahrung im IT-Audit Bereich und das Befolgen des Verhaltenscodex der ISACA gebunden.

Inhaltlich werden beim CISA-Examen Fragen aus den folgenden Bereichen gestellt:

- IT Management, Planung und Organisation
- Technische Infrastruktur
- IT-Sicherheit
- Notfallplanung
- Systementwicklung, -auswahl, -einführung und –wartung
- Geschäftsprozessanalyse und Risikomanagement

Momentan gibt es weltweit ca. 23.000 Personen, die berechtigt sind, den CISA Titel zu führen.

A.5 Zuordnung der I- und E-Module zu den Modulen des OSSTMMs

Die unten stehenden Tabellen zeigen die Zuordnung der I- bzw. E-Module zu den Modulen des OSSTMM 2.0 RC 6 [Herzog02]. Da das OSSTMM keine Unterscheidung zwischen verdeckten und offensichtlichen Tests enthält bzw. aufgrund von Zusammenfassungen einzelner OSSTMM Module ist keine 1:1 bzw. keine N:1 / 1:N Zuordnung möglich, sondern eine N:M Zuordnung erforderlich.

A.5.1 Zuordnung der Module zur Informationsbeschaffung

Nr.	*Modulbezeichnung*	*OSSTMM 2.0 RC 6*
I 1	Auswertung öffentlich zugänglicher Daten	M 2.03 Document Grinding
I 2	Verdeckte Abfragen von Netzwerkbasis-informationen	M 1.01 Network Surveying
I 3	Offensichtliche Abfragen von Netzwerkbasis-informationen	M 1.01 Network Surveying
I 4	Verdeckte Durchführung von Portscans	M 1.02 Port Scanning
I 5	Offensichtliche Durchführung von Portscans	M 1.02 Port Scanning
I 6	Identifikation von Anwendungen	M 1.03 Services Identification M 1.06 Internet Application Testing
I 7	Identifikation von Systemen	M 1.04 System Identification
I 8	Verdeckte Identifikation der Router	M 1.07 Router Testing
I 9	Offensichtliche Identifikation der Router	M 1.07 Router Testing
I 10	Verdeckte Identifikation der Firewalls	M 1.09 Firewall Testing
I 11	Offensichtliche Identifikation der Firewalls	M 1.09 Firewall Testing
I 12	Recherche nach Schwachstellen	M 1.05 Vulnerability Research
I 13	Identifikation von Anwendungsschnittstellen	M 1.06 Internet Application Testing
I 14	Sammlung von Informationen für Social-Engineering	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
I 15	Sammlung von Informationen für computerbasiertes Social-Engineering	-

Nr.	*Modulbezeichnung*	*OSSTMM 2.0 RC 6*
I 16	Sammlung von Informationen für persönliches Social-Engineering	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
I 17	Überprüfung der drahtlosen Kommunikation (nur scannend)	M 4.01 Wireless Networks Testing M 4.02 Cordless Communications Testing M 4.04 Infrared Systems Testing
I 18	Test der Telefonanlage (Identifikation)	M 5.01 PBX Testing
I 19	Test des Voicemailsystems (Identifikation)	M 5.02 Voicemail Testing
I 20	Test des Faxsystems (Identifikation)	M 5.03 FAX Review
I 21	Analyse der physischen Umgebung	M 6.05 Location Review
I 22	Identifikation von Zutrittskontrollen	M 6.01 Access Controls Testing]M 6.03 Monitoring Review
I 21	Analyse der physischen Umgebung	M 6.05 Location Review

A.5.2 Zuordnung der Module für aktive Eindringversuche

Nr.	*Modulbezeichnung*	*OSSTMM 2.0 RC 6*

Nr.	*Modulbezeichnung*	*OSSTMM 2.0 RC 6*
E 1	Verdeckte Verifikation tatsächlicher Schwachstellen	M 1.05 Vulnerability Research
E 2	Offensichtliche Verifikation tatsächlicher Schwachstellen	M 1.05 Vulnerability Research
E 3	Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen	M 1.06 Internet Application Testing
E 4	Verdeckter Test der Router	M 1.07 Router Testing
E 5	Offensichtlicher Test der Router	M 1.07 Router Testing
E 6	Test von Vertrauensbeziehungen zwischen Systemen	M 1.08 Trusted Systems Testing
E 7	Verdeckter Test der Firewall von außen	M 1.09 Firewall Testing
E 8	Offensichtlicher Test der Firewall von außen	M 1.09 Firewall Testing
E 9	Beidseitiger Test der Firewall	M 1.09 Firewall Testing
E 10	Test des IDS-Systems	M 1.10 IDS Testing
E 11	Abhören von Passwörtern	M 1.12 Password Cracking
E 12	Test von Passwörtern	M 1.12 Password Cracking
E 13	Test von „Denial-of-Service“ Anfälligkeit	M 1.13 Denial of Service Testing
E 14	Computerbasiertes Social-Engineering	-
E 15	Direktes, persönliches Social-Engineering mit physischem Zutritt	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
E 16	Indirektes, persönliches Social-Engineering ohne physischen Zutritt	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
E 17	Überprüfung der drahtlosen Kommunikation	M 4.01 Wireless Networks Testing M 4.02 Cordless Communications Testing M 4.04 Infrared Systems Testing

Nr.	*Modulbezeichnung*	*OSSTMM 2.0 RC 6*
E 18	Test der administrativen Zugänge zur Telefonanlage	M 5.01 PBX Testing
E 19	Test des Voicemailsystems	M 5.02 Voicemail Testing
E 20	Test der administrativen Zugänge zum Faxsystems	M 5.03 FAX Review
E 21	Test von Modems	M 5.04 Modem Testing
E 22	Aktiver Test der Zutrittskontrollen	M 6.01 Access Controls Testing
E 23	Überprüfung der Eskalationsprozeduren	M 6.03 Monitoring Review M 6.04 Alarm Response Review

A.6 Checklisten und Vorlagen zur Dokumentation

A.6.1 Checkliste zur Abarbeitung der I-Module

Nr.	*Modulbezeichnung*	*Ref.-Nr.*	*erledigt*
I 1	Auswertung öffentlich zugänglicher Daten		☐
I 2	Verdeckte Abfragen von Netzwerkbasis-informationen		☐
I 3	Offensichtliche Abfragen von Netzwerkbasis-informationen		☐
I 4	Verdeckte Durchführung von Portscans		☐
I 5	Offensichtliche Durchführung von Portscans		☐
I 6	Identifikation von Anwendungen		☐
I 7	Identifikation von Systemen		☐
I 8	Verdeckte Identifikation der Router		☐
I 9	Offensichtliche Identifikation der Router		☐
I 10	Verdeckte Identifikation der Firewalls		☐
I 11	Offensichtliche Identifikation der Firewalls		☐
I 12	Recherche nach Schwachstellen		☐
I 13	Identifikation von Anwendungsschnittstellen		☐
I 14	Sammlung von Informationen für Social-Engineering		☐
I 15	Sammlung von Informationen für computerbasiertes Social-Engineering		☐
I 16	Sammlung von Informationen für persönliches Social-Engineering		☐
I 17	Überprüfung der drahtlosen Kommunikation (nur scannend)		☐
I 18	Test der Telefonanlage (Identifikation)		☐
I 19	Test des Voicemailsystems (Identifikation)		☐
I 20	Test des Faxsystems (Identifikation)		☐

Nr.	*Modulbezeichnung*	*Ref.-Nr.*	*erledigt*
I 21	Analyse der physischen Umgebung		☐
I 22	Identifikation von Zutrittskontrollen		☐

A.6.2 Checkliste zur Abarbeitung der E-Module

Nr.	*Modulbezeichnung*	*Ref.-Nr.*	*erledigt*
E 1	Verdeckte Verifikation tatsächlicher Schwachstellen		☐
E 2	Offensichtliche Verifikation tatsächlicher Schwachstellen		☐
E 3	Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen		☐
E 4	Verdeckter Test der Router		☐
E 5	Offensichtlicher Test der Router		☐
E 6	Test von Vertrauensbeziehungen zwischen Systemen		☐
E 7	Verdeckter Test der Firewall von außen		☐
E 8	Offensichtlicher Test der Firewall von außen		☐
E 9	Beidseitiger Test der Firewall		☐
E 10	Test des IDS-Systems		☐
E 11	Abhören von Passwörtern		☐
E 12	Test von Passwörtern		☐
E 13	Test von „Denial-of-Service“ Anfälligkeit		☐
E 14	Computerbasiertes Social-Engineering		☐
E 15	Direktes, persönliches Social-Engineering mit physischem Zutritt		☐
E 16	Indirektes, persönliches Social-Engineering ohne physischen Zutritt		☐
E 17	Überprüfung der drahtlosen Kommunikation		☐
E 18	Test der administrativen Zugänge zur Telefonanlage		☐
E 19	Test des Voicemailsystems		☐
E 20	Test der administrativen Zugänge zum Faxsystems		☐

Nr.	*Modulbezeichnung*	*Ref.-Nr.*	*erledigt*
E 21	Test von Modems		☐
E 22	Aktiver Test der Zutrittskontrollen		☐
E 23	Überprüfung der Eskalationsprozeduren		☐

A.6.3 Vorlage zur Sammlung von Serverinformationen

DNS-Name	
IP-Adresse	
Rolle	
Betriebssystem	

Port	**Protokoll**	**Anwendung**	**pot. Schwachstelle**

Sonstige Informationen

A.6.4 Vorlage zur Sammlung von Social-Engineering Informationen

Name	
Funktion	
E-Mail	
Telefon	

Beschreibung des Angriffs	
Ergebnis	

A.6.5 Vorlage zur Sammlung von weiteren Informationen

Bereich / Modul	

Beschreibung der Prüfungs-hand-lung	
Ergebnis	

A.7 Tools

In folgender Tabelle befindet sich eine Auflistung von Hacker- / Security-Tools, die im Rahmen von Penetrationstests eingesetzt werden können. Sofern nicht anders vermerkt, handelt es sich dabei um freie Software. Die Auflistung stellt keinen Vergleich über die enthaltenen Funktionalitäten der Tools dar und erhebt keinen Anspruch auf Vollständigkeit.

Name	*Besonderheiten*	*Plattform*	*Bezugsquelle*
Portscanner			
7th Sphere Port-scanner	einfach zu bedienender Portscanner	Windows	http://www.computech.ch
Nmap	Portscanner mit erweiterter Funktio-nalität, wie Stealth-Scans oder System-erkennung	Unix, Windows	http://www.insecure/nmap
Strobe	schneller TCP-Portscanner	Unix	ftp://suburbia.net/pub
Super Scan	Portscanner mit leicht zu bedienender Benutzeroberfläche	Windows	http://www.computech.ch
Schwachstellen-Scanner			
Cerberus Internet Scanner	Schwachstellen-Scanner, der als Freeware Version und als kommerzielle Version mit erweitertem Funktionsum-fang erhältlich ist.	WinNT, Win2000	http://www.cerberus-infosec.co.uk/cis.shtml
Happy Browse /THC	Schwachstellen-Scanner, der eine Liste mit potenziellen Schwachstellen erzeugt, jedoch ohne Hinweise auf deren Ausnutzung	Windows	http://www.pimmel.com/thcfiles.php3
ISS Internet Scan-ner	kommerzieller Schwachstellen-Scanner	Win2000, WinXP	http://www.iss.net
Nessus	Schwachstellen-Scanner, der aus einer Client- und Serverkomponente besteht	Unix, Windows	http://www.nessus.org
Saint	kommerzieller Schwachstellen-Scanner	Unix	http://www.wwdsi.com
SARA	Freeware-Version des kommerziellen Schwachstellen-Scanners Saint	Unix	http://www-arc.com/sara
SATAN	Vulnerability-Scanner der ersten Generation, mittlerweile veraltet und nicht mehr weiterentwickelt worden	Unix	http://www.fish.com/satan
Xscan	Schwachstellen-Scanner, der sowohl von der Kommandozeile als auch über	Windows	http://www.xfocus.org/programs.php

Name	*Besonderheiten*	*Plattform*	*Bezugsquelle*
	eine GUI zu bedienen ist.		
Wardialer			
Phonesweep	kommerzieller Wardialer, erfordert spezielle Hardware	n.a.	http://sandstorm.net/products/phonesweep
THC Scan	gebräuchlicher Wardialer unter DOS/Windows	DOS	http://www.thehackerschoice.com
ToneLoc	etwas veralteter Wardialer	DOS	
CGI-Scanner			
Whisker	Tool zum Aufspüren von Sicherheitslücken in CGI-Skripten	Unix	http://sourceforge.net/projects/whisker
WLAN Scanner			
Kismet	Tool zum Auffinden und Abhören von WLANs	Unix	http://www.kismetwireless.net
Net Stumbler	Tool zum Auffinden von WLANs	Windows	http://www.netstumbler.com
Weitere Scan-Tools			
Cheops	liefert eine graphische Darstellung des gescannten Netzwerks	Unix	ftp://ftp.marko.net/pub/cheops
Firewalk	Tool zum Testen von Firewallregeln	Unix	http://www.packetfactory
Languard	Portscanner mit vielen weitern Funktionen	Win95, WinNT	http://www.gfi.com/downloads
Sam Spade	universell einsetzbares Tool zu Informationsgewinnung, u.a. Whois und DNS-Abfragen	Windows	http://www.samspade.org
Visualroute	liefert eine graphische Übersicht der Routenverfolgung	Unix, Windows	http://www.visualroute.com
What´s running	liefert Informationen über die auf einem Zielrechner laufende Software	Windows	http://www.woodstone.nu/whats
LAN Sniffer			
Angst	ermöglicht Sniffen in geswitchten Netzen	FreeBSD	http://wiretapped.net
Dsniff	Dsniff beinhaltet eine Sammlung von Programmen die es auch in geswitchten Netzen ermöglichen, Netzwerkverkehr abzuhören	Unix	http://www.monkey.org
Ethereal	Packet-Sniffer, der auch Informatio-	Windows,	http://www.ethereal.com

Name	*Besonderheiten*	*Plattform*	*Bezugsquelle*
	nen der Anwendungsschicht interpretieren kann	Unix	
Sniffit	Tool, das speziell darauf ausgelegt ist, Anwendungsdaten und Passwörter aufzuzeichnen	Unix	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
Snort	Intrusion Detection System, das über eine Sniffer-Komponente verfügt	Windows, Unix	http://www.snort.org
Tcpdump	Packet-Sniffer für OSI-Schicht 1 bis 4	Unix	http://www.tcpdump.org
Windump	Windows-Version von Tcpdump	Windows	http://winpcap.polito.it
WLAN Sniffer			
AirSnort	Dieses Tool ermöglicht die Datenaufzeichnung in WLANS	Linux	http://sourceforge.net/projects/airsnort
WEPCrack	Dieses Tool kann zum Cracken von Schlüsseln in WLANS eingesetzt werden	Linux	http://sourceforge.net/projects/wepcrack
Passwort Cracker			
Brutus	ermöglicht das Cracken von Telnet/FTP/Netbios/POP3-Passwörtern	Windows	http://hobbie.net/brutus/brutus-download.html
Crack	ermöglicht das Cracken von Unix-Passwörtern	Unix	http://www.users.dircon.co.uk/~crypto/
John the Ripper	Tool zu Cracken von NT und Unix Passwörtern	Unix, DOS, Windows	http://www.openwall.com/john
L0pht Crack	ermöglicht das Cracken von Windows-Passwörtern	Windows	http://www.atstake.com
Web Cracker	ermöglicht das Überwinden von Web-Authentifizierungen	Windows	http://www.packetstormsecurity.org
Angriffs-Tools			
Fragrouter	Tool zum fragmentieren von Paketen	Unix	http://www.packetstormsecurity.com
Hping	ermöglicht das Testen von Firewall-Regeln, viele weitere Optionen	Unix	http://www.hping.org
Hunt	Tool zum Durchführen eines Session Hijacking Angriffes	Unix	http://www.wiretapped.net
IRPAS	Sammlung von Programmen	Unix	http://phenoelit.de
Jolt2	Tool zum Durchführen einer DoS-Attacke	Unix	http://www.securiteam.com/exploits/Jolt2_-_a_new_Windows_DoS_attack.html

Name	*Besonderheiten*	*Plattform*	*Bezugsquelle*
Nemesis	Sammlung von Tools, die es ermöglichen, Datenpakete zu manipulieren	Unix	http://the.wiretapped.net
RafaleX	Packet Builder, der es ermöglicht IP/TCP/UDP Pakete zu manipulieren	Windows	http://www.packx.net/packx
Stacheldraht	Tool zum Durchführen einer verteilten DoS-Attacke (Ddos-Attacke)	Unix	
TFN2000	Tool zum Durchführen einer verteilten DoS-Attacke (Ddos-Attacke)	Windows, Unix	
Trin00	Tool zum Durchführen einer verteilten DoS-Attacke (Ddos-Attacke)	Unix	
Trojanische Pferde			
Back Orifice	Tool, das eine Remote-Bedienung eines PCs ermöglicht	Windows	http://www.cultdeadcow.com
Netbus	Tool, das eine Remote-Bedienung eines PCs ermöglicht	Windows	http://www.windowsecurity.com
Sub Seven	Tool, das eine Remote-Bedienung eines PCs ermöglicht	Windows	http://www.subseven.ws
Weitere Tools			
Datapipe.c	Tool, mit dem Verbindungen umgeleitet und somit Firewallregeln umgangen werden können.	Unix	http://packetstormsecurity.nl/unix-exploits/tcp-exploits
Fpipe	ermöglicht die Umleitung von Verbindungen zu einem anderen Port und dadurch die Umgehung einer Firewall	Windows	http://www.networkingfiles.com
Netcat	Universell einsetzbares Tool zur Manipulation von TCP und UDP-Verbindungen	Windows, Unix	http://www.atstake.com