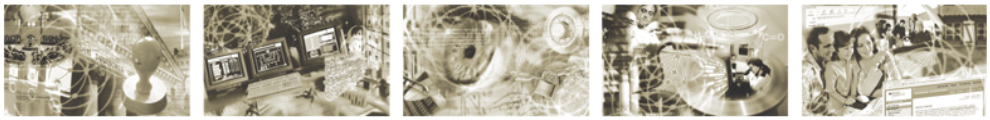
Bundesamt
für Sicherheit in der
Informationstechnik



Ein Praxis-Leitfaden für IS-Penetrationstests

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

Stand: Version 1.2 (November 2016)

Inhaltsverzeichnis

1 Einleitung

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

Im Folgenden wird der IT-Sicherheits-Penetrationstest (IS-Penetrationstest) als ein bewährtes Mittel hierzu beschrieben. Das vorliegende Dokument soll als Leitfaden für die Beauftragung von IS-Penetrationstests dienen und die Rahmenbedingungen bei der Durchführung erläutern.

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

1.1 Adressatenkreis

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

Auch Anbieter von IS-Penetrationstests (im Folgenden Prüfer genannt) seien angeregt, das Dokument zu lesen und ihre eigene Vorgehensweise mit der beschreibenen zu vergleichen.

1.2 Zielsetzung

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

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

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

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

Das BSI empfiehlt...

1.3 Begriffsbestimmung IS-Penetrationstest

Ein IS-Penetrationstest ist ein erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.

Im Detail werden dabei die installierten IT-Anwendungen (Webanwendung, Mailserver, etc.) beziehungsweise die zugrunde liegenden Trägersysteme (Betriebssystem, Datenbank, etc.) überprüft.

Typische Ansatzpunkte für einen IS-Penetrationstest sind:

- Netzkoppelelemente (Router, Switches, Gateways)
- Sicherheitsgateways (Firewall, Paketfilter, Intrusion Detection System, Virenscanner, Loadbalancer etc.)
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme, etc.)
- Telekommunikationsanlagen
- Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop)
- Clients
- Drahtlose Netze (WLAN, Bluetooth)
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)

Üblicherweise werden IS-Penetrationstests in Blackbox-Tests und Whitebox-Tests unterteilt. Bei einem Blackbox-Test stehen den Prüfern lediglich die Adressinformationen des Zieles zur Verfügung. Mittels der Vorgehensweise "Blackbox-Test" soll der Angriff eines typischen Außentäters simuliert werden, der nur unvollständige Kenntnisse über das Zielsystem hat. Dagegen verfügen die Prüfer bei einem Whitebox-Test über umfangreiche Informationen über die zu testenden Systeme. Dazu gehören beispielsweise Informationen über IP-Adressen des internen Netzes, die eingesetzte Soft- und Hardware etc. Diese Angaben werden den Prüfern zuvor vom Auftraggeber mitgeteilt.

Das BSI empfiehlt, grundsätzlich Whitebox-Tests durchzuführen, da bei einem Blackbox-Test aufgrund nicht vorliegender Informationen Schwachstellen übersehen werden können. Es besteht die Gefahr, dass im Rahmen eines Blackbox-Tests Szenarien wie der Angriff eines informierten Innentäters nicht berücksichtigt werden. Zusätzlich besteht bei einem Blackbox-Test ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden zu verursachen. Darüber hinaus ist der Aufwand bei einem Blackbox-Test wesentlich größer als

bei einem Whitebox-Test. Den Prüfern sollten daher nach Möglichkeit alle für die Testdurchführung notwendigen Informationen über die zu testenden Systeme zur Verfügung gestellt werden.

IS-Penetrationstests können in unterschiedlicher Tiefe durchgeführt werden. Zu vermeiden sind dabei destruktive Tests, das heißt Tests, bei denen die Zielsysteme zu Schaden kommen könnten.

Ein Weg, vorhandene Schwachstellen nachzuweisen, ist, mit so genannten technischen Sicherheitsaudits stichprobenartig sicherheitsrelevante Konfigurationen und Regelwerke der eingesetzten IT-Systeme zu untersuchen und anhand der Versionen und Patchstände Rückschlüsse auf Schwachstellen zu ziehen.

Darüber hinaus können mit einem automatisierten Schwachstellenscanner Gefährdungen in den getesteten IT-Systemen aufgezeigt werden.

Das BSI empfiehlt grundsätzlich eine moderate Angriffsstärke zu wählen. Ein IS-Penetrationstest soll dafür so dimensioniert werden, dass Schwachstellen zwar nachgewiesen, aber nur aktiv ausgenutzt werden, wenn es nicht vermeidbar ist und die Exploits ausreichend getestet wurden.

1.4 Abgrenzungen

1.4.1 Grenzen des Leitfadens

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

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

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

1.4.2 Abgrenzungen für IS-Penetrationstests

Ein IS-Penetrationstest ersetzt keine Qualitätssicherung von neuen oder geänderten IT-Anwendungen oder IT-Systemen. Die erforderliche Qualitätssicherung muss in jeder Institution in den Lebenszyklus der eingesetzten Hard- und Software integriert sein.

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

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

Die meisten IS-Penetrationstests sind sowohl zeitlich als auch von ihrem Umfang her begrenzt und beziehen sich nur auf die zu erwartenden Hauptangriffsziele des Prüfobjekts. Daneben können aber auch weitere Schwachstellen in den IT-Systemen vorhanden sein.

Der IS-Penetrationstest, *wie das BSI ihn durchführt*, beinhaltet weiterhin keinerlei Elemente des Social Engineering. Reale Angriffe würden höchstwahrscheinlich über Elemente des Social Engineering gestartet werden oder solche beinhalten. Bei Social Engineering Angriffen werden über die Gutgläubigkeit der Mitarbeiter, aber auch über Informationen, die im Internet (beispielsweise Social Media oder Foren) frei verfügbar sind, Kenntnisse über die Strukturen einer Institution und auch über deren IT-Systeme zusammengetragen, um mit weiteren Angriffen gezielt darauf aufbauen zu können. Es wird empfohlen, dass Institutionen ihre Mitarbeiter in einem hohen Maß für solche Angriffsmethoden sensibilisieren. Die Simulation eines Social Engineering-Angriffs kann zwar auf der einen Seite die Aufmerksamkeit für solche Methoden stark verbessern, die Erfahrung zeigt aber, dass sich immer wieder einzelne Mitarbeiter durch nachgestellte Social Engineering Aktionen bloßgestellt sehen, wenn diese bei ihnen erfolgreich waren. Um dies zu vermeiden, sollten solche Tests nur unter genau definierten Rahmenbedingungen mit Einbeziehung der Personalvertretung und mit darauf trainierten Spezialisten durchgeführt werden.

1.4.3 Abgrenzung zu anderen IT-Sicherheitstests

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

IS-Revisionen

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

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

Code-Rreview

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

IS-Webcheck

Ein IS-Webcheck ist ein Spezialfall eines IS-Penetrationstests. Mit einem IS-Webcheck wird der Sicherheitsstand einer Internetpräsenz einer Institution geprüft. Hierbei werden die Webanwendungen größtenteils durch den Einsatz automatisierter Methoden über das Internet geprüft.

2 Organisatorische Voraussetzung für einen IS-Penetrationstest

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

2.1 Anforderung an die Institution

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

2.1.1 Motivation für einen IS-Penetrationstest

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

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

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

2.1.2 Rahmenbedingungen für einen IS-Penetrationstest

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

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

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

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

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

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

Wird ein Webauftritt untersucht, sollte zunächst die Webanwendung ohne vorgeschaltetes Sicherheitsgateway mit einem IS-Webcheck [3] untersucht werden. Hierbei wird überprüft, ob gängige Sicherheitslücken in der IT-Anwendung geschlossen sind und eine gute Eingabevalidierung vorliegt. Das Sicherheitsgateway sowie weitere Schnittstellen zu dem Webauftritt werden im letzten Schritt dann durch einen IS-Penetrationstest überprüft.

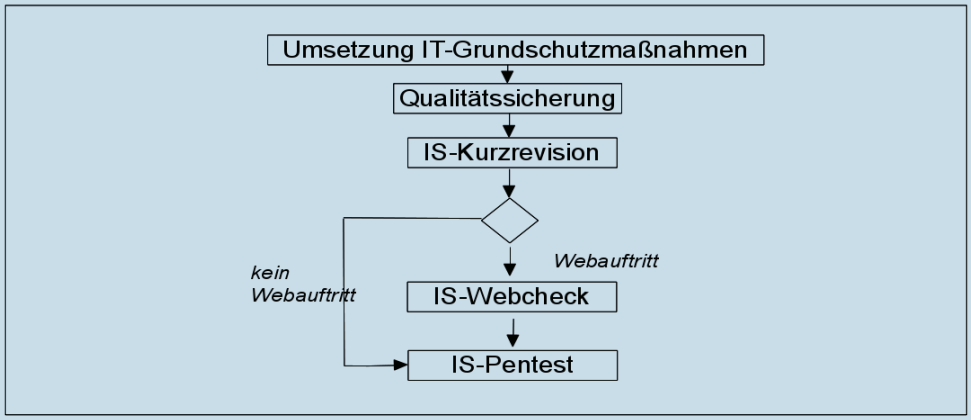


Abbildung 1: Reihenfolge der Sicherheitsmaßnahmen

2.2 Anforderungen an einen Prüfer

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

2.2.1 Fachliche Anforderungen

Die Prüfer müssen umfangreiche fachliche Kenntnisse haben. Werden die weiter unten angegebenen Zertifikate vorgelegt, so kann von einer breiten fachlichen Qualifikation ausgegangen werden. Ohne die Vorlage von Zertifikaten sollte zunächst anhand des Prüfobjekts entschieden werden, welche Qualifikationen erforderlich sind. Ein erfolgreicher Prüfer im Webanwendungsbereich ist nicht zwangsläufig auch dafür geeignet, das IT-Sicherheitsgateway zu untersuchen.

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

- Systemadministration
- Netzwerkprotokolle
- Programmiersprachen
- IT-Sicherheitsprodukte (IT-Sicherheitsgateways, Intrusion-Detection-Systeme, etc.)
- Anwendungssysteme
- Netzkomponenten

Es ist hilfreich, wenn ein Prüfer selbst schon im Bereich Systemadministration oder Programmierung gearbeitet hat, da er hierdurch Erfahrung mit allen möglichen Fehlerquellen mitbringt.

2.2.2 Weitere Fähigkeiten

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

Ein Prüfer sollte folgende Qualitäten besitzen:

- organisatorische Fähigkeiten
- zielorientiertes Denken und Handeln
- Überzeugungsfähigkeit
- schnelle Auffassungsgabe
- gesundes Urteilsvermögen

- analytische Fähigkeiten
- Teamfähigkeit
- Belastbarkeit
- Sachlichkeit insbesondere bei heiklen Sachverhalten

Die aufgezählten Fähigkeiten lassen sich nicht einfach nachweisen. Bei der Beauftragung eines Prüfers muss sich die Institution daher bei diesen Punkten teilweise auf die eigene Intuition und die Erfahrungen mit dem Auftragnehmer verlassen.

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

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

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

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

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

2.2.3 Technische Qualifikation / Zertifikate

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

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

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

2.2.4 Verwendete Tools

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

2.3 Weitere Rahmenbedingungen

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

Verträge

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

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

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

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

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

NDA (Non Disclosure Agreement)

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

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

Speicherzeit von Daten

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

Datenschutz

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

Geheimschutz

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

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

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

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

Wartung der IT-Systeme

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

3 Fachliche Voraussetzungen für einen IS-Penetrationstest

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

3.1.1 Festlegung des Prüfobjekts zwischen Prüfer und Institution

Die Institution und der Prüfer sollten genau festlegen, welche Bereiche getestet werden. Hierbei empfiehlt es sich, auf Basis der identifizierten Bedrohungslage und dem Schutzbedarf der Geschäftsprozesse und Informationen diejenigen IT-Systeme in den Fokus zu nehmen, die besonders bedroht oder geschäftskritisch sind. Außerdem sollte aus Angreifersicht geschaut werden, wo Schnittstellen auf die IT-Systeme sind, über die Angreifer eindringen könnten.

Übliche Prüfobjekte sind u.a.

- Netzkoppelelemente (Router, Switches, Gateways)
- Sicherheitsgateways (Firewalls, Paketfilter, Intrusion Detection System, Virenscanner etc.)
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme etc.)
- Telekommunikationsanlagen
- Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop)
- Clients
- Drahtlose Netze (WLAN, Bluetooth)
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)

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

Wenn eine Institution präventiv einen IS-Penetrationstest durchführen möchte, so fällt es oft schwer, das Prüfobjekt einzugrenzen. Die Institution möchte jede Angriffsmöglichkeit identifizieren und beseitigen. Dies ist allerdings sehr zeitaufwendig und teuer. Oft steht auch kein Prüfer für eine so lange Zeitspanne zur Verfügung. Daher sollte überlegt werden, wo ein Angriff am wahrscheinlichsten ist und die identifizierten Schnittstellen zuerst getestet werden. Es können in der Folgezeit sukzessive weitere IS-Penetrationstests auf weitere Schnittstellen durchgeführt werden. Da Prüfer keine Qualitätssicherung übernehmen können und Betriebsblindheit vermieden werden muss, sollten die gleichen Prüfobjekte nicht mehrfach von denselben Prüfern geprüft werden.

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

3.1.2 Festlegung des Prüfumfangs

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

Hierbei werden folgende Aspekte vereinbart:

- Prüftiefe
- Prüfort
- Prüfzeitraum
- Prüfbedingungen

Prüftiefe

Die IS-Penetrationstests können in unterschiedlicher Tiefe durchgeführt werden. Wird vereinbart, ein *technisches Sicherheitsaudit* durchzuführen, so wird anhand der Versionen der eingesetzten IT-Anwendungen und den vorhandenen Konfigurationen auf mögliche Schwachstellen hingewiesen. Der Prüfer bedient die IT-Systeme hierbei nicht selbst, sondern lässt sich von einem Administrator vor Ort zeigen, welche Versionen in welcher Konfiguration eingesetzt werden und welche Härtungsmaßnahmen getroffen wurden. Es wird anhand der vorgefundenen Versionen und umgesetzten Sicherheitsmaßnahmen auf mögliche Schwachstellen geschlossen.

Ein *nicht invasiver Schwachstellenscan* ist die nächstmögliche Prüftiefe. Hierbei scannt der Prüfer zusätzlich zu dem technischen Sicherheitsaudit mit eigenen Geräten im Netz nach Schwachstellen. Er setzt hierzu Schwachstellenscanner ein, nutzt die Schwachstellen aber nicht aus. Hierdurch kann beobachtet werden, wie sich ein fremdes Gerät im Netz verhält und was es sieht. Bei automatisierten Methoden ist der Nachteil, dass möglicherweise viele "False Positives" gemeldet werden, also fälschlich Sicherheitslücken identifiziert werden, die nicht vorhanden sind. Die meisten Schwachstellenscanner entscheiden beispielsweise anhand der Versionen der eingesetzten Betriebssysteme und Anwendungen, ob eine Schwachstelle vorliegt. Es muss jedoch berücksichtigt werden, dass in einigen Fällen aus Kompatibilitätsgründen zu anderen Anwendungen bewusst alte Versionen eingesetzt werden, die aber gepatched sind.

In der nächsten Prüftiefe beim *invasiven Schwachstellenscan* werden zusätzlich so genannte Exploits eingesetzt. Das sind Programme, die eigens zum Ausnutzen von bekannten Schwachstellen geschrieben wurden. Hierdurch wird nachgewiesen, dass ein IT-System angreifbar ist. Der Nachteil ist, dass Exploits die IT-Systeme beeinträchtigen können.

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

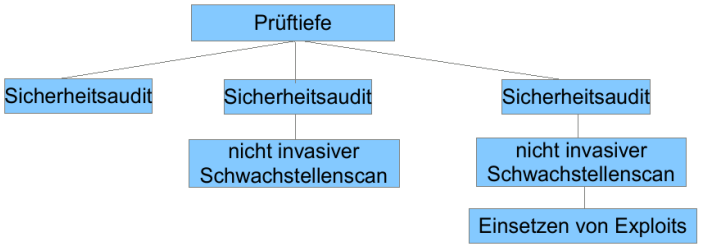


Abbildung 2: Prüftiefe

Prüfort

Schließlich muss der Ort festgelegt werden, wo der IS-Penetrationstest stattfindet. Es muss geklärt werden, ob es möglich ist, eine IT-Anwendung über das Internet zu testen, oder ob der IS-Penetrationstest vor Ort in der zu prüfenden Institution stattfindet. Außerdem ist zu klären, ob der IS-Penetrationstest im Rechenzentrum, bei der Institution oder über eine Fernwartung durchgeführt wird.

Ein geschulter Prüfer profitiert von den Gesprächen mit den Verantwortlichen vor Ort und findet manchmal gerade über die Gespräche und die Eindrücke vor Ort die Schwachstellen im IT-System. Daher wird empfohlen, wenn möglich, die IS-Penetrationstests vor Ort durchzuführen. Es sei denn, es handelt sich bei dem Prüfobjekt um eine Webanwendung, die über das Internet getestet werden soll, oder die IT-Systeme stehen an einem entfernten Ort, für den die Reisekosten die geplanten Kosten des Tests überschreiten würden.

Der Vorteil, einen Test im Rechenzentrum durchzuführen, ist, dass der Prüfer auch andere Eindrücke gewinnt, beispielsweise durch die Art der Verkabelung.

Prüfbedingungen

Wenn der Ort des IS-Penetrationstests festgelegt ist, muss genau geplant werden, welche Gegebenheiten der Auftraggeber für den Prüfer einplanen muss. Der Prüfer muss im Prüfzeitraum in der zu prüfenden Institution einen geeigneten Arbeitsplatz haben. Wenn er einen eigenen Laptop als Prüfwerkzeug in das Netz einbringt, so müssen hierfür die nötigen Freigaben geschaffen werden. Beispielsweise kann es sein, dass Prüfgeräte (beispielsweise die MAC-Adresse) für das Netz zugelassen werden müssen.

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

Wenn das Produktivsystem getetet wird, kann überlegt werden, ob der Prüfzeitraum auf einen Zeitraum gelegt wird, in dem wenig Beeinträchtigung für den regulären Betrieb zu erwarten sind.

Hierbei muss allerdings beachtet werden, dass dann gegebenenfalls der notwendige Datenverkehr für die Tests fehlen könnte.

Wenn über das Internet getestet wird, so muss der Zugriff der Prüfer auf die zu testenden IT-Systeme freigeschaltet sein. Eventuelle Blockaden des Sicherheitsgateways müssen für den Prüfzeitraum abgeschaltet werden. Dies dient dazu, exakte Ergebnisse bzgl. der getesteten IT-Anwendung zu erhalten. Wenn das Sicherheitsgateway zusätzliche Absicherungen bereithält, ist das für den Betrieb gut. Ein genaues Prüfergebnis, wo welche Schwächen zu beseitigen sind, kann der Prüfer leichter und damit kostengünstiger erzeugen, wenn er die IT-Systeme getrennt voneinander testet. Die Funktion des Sicherheitsgateways sollte dann in einem separaten IS-Penetrationstest getestet werden.

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

Prüfzeitraum

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

3.1.3 Dokumentation

Damit die Prüfer bei einem Whiteboxtest einen schnellen Überblick über die zu testenden Prüfobjekte erhalten, sollten die im Folgenden aufgelisteten Unterlagen vom Auftraggeber zur Verfügung gestellt werden.

- **Netzpläne**

  In Netzplänen wird das Prüfobjekt grafisch innerhalb der Umgebung, in der es sich befindet, skizziert. Wichtig ist, dass alle Kommunikationsverbindungen zu anderen IT-Systemen und IT-Anwendungen identifiziert werden können und die Netzkomponenten erkennbar sind. Zur Erleichterung der Arbeit vor Ort sollten die verwendeten IP-Adressen eingezeichnet werden. Alle Schnittstellen für Mensch und Maschinen sollten klar erkennbar sein. Schnittstellen, welche auch von Externen zu erreichen sind (beispielsweise Anbindung ans Internet, WLAN, Netzwerkdosen in Besprechungsräumen), sollten besonderes gekennzeichnet werden.

- **Beschreibung des Prüfobjekts**

  Eine Dokumentation des Prüfobjekts sollte vorliegen. Hierbei soll beschrieben werden, wofür das Prüfobjekt benötigt wird. Die Dokumentation soll mindestens beschreiben, welche Teilnehmer Zugriff auf das Objekt besitzen, zu welchen Zeiten Zugriffe erfolgen,

welche Daten personenbezogen sind oder ggf. nach Geheimschutz zu behandeln sind sowie welche IT-Systeme für das Funktionieren der IT-Anwendung wichtig sind.

IT-Anwendungen sollen in klar abgegrenzte Funktionen unterteilt und erläutert werden. Spezielle Sicherheitsmaßnahmen bezüglich der IT-Anwendung sollen verständlich beschrieben sein.

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

  Darüber hinaus sollten alle IT-Systeme mit der grundsätzlichen Beschreibung der Härtungsmaßnahmen dokumentiert sein. Alleine die Auseinandersetzung der Institution mit diesem Thema führt dazu, dass unerwünschte Dienste bereits identifiziert und abgeschaltet sind.

  Da die meisten IT-Systeme aus laufenden Prozessen bestehen, die beispielsweise durch regelmäßige Updates veränderlich bleiben, genügt für die Vorbereitung der IS-Penetrationstests ein Status-quo-Abbild der IT-Systeme. Bei Servern bedeutet das, dass eine Liste der installierten Programme und Dienste erstellt wird und die laufenden Prozesse dokumentiert werden. Für die Einschätzung von Netzkomponenten sind Konfigurationsdateien und Regelwerke wichtig.

- **Beschreibung der Kommunikationsverbindungen**

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

Zusätzlich kann es hilfreich sein, ein Sicherheitskonzept mit Beschreibung der Fachverfahren und Bewertung des Schutzbedarfs beizufügen.

Es ist nach ISO 27001 bzw. IT-Grundschutz grundsätzlich empfohlen, diese Dokumente vorzuhalten, um einen sicheren Betrieb nachzuweisen. Die Dokumente sollten erstellt werden, beispielsweise um Fehlerquellen im laufenden Betrieb schnell finden zu können und Vertretungsregelungen zu garantieren.

3.1.4 Verantwortlichkeiten

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

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

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

4 Ablauf eines IS-Penetrationstests

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

4.1.1 Einarbeitung der Prüfer

Das erste Arbeitspaket des IS-Penetrationstests sollte der Einarbeitung der Prüfer dienen. Ein versierter Prüfer benötigt möglicherweise weniger Zeit, wenn er die Art der IT-Systeme vor Ort gut kennt. Für ausgefallenere IT-Systeme wird meist mehr Zeit benötigt. Die Institution muss den Prüfern für die Einarbeitung eine ausführliche Dokumentation (siehe Kapitel 3.1.3) zur Verfügung stellen.

4.1.2 Test des Prüfobjekts

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

- Anfangsgespräch
- Einrichten der Arbeitsumgebung
- Praktische Prüfung
- Abschlussgespräch

Je nach Umfang des Tests können außerdem verschiedene Zwischengespräche notwendig sein oder einzelne Pakete wie das Einrichten der Arbeitsumgebung und die praktische Prüfung mehrfach durchgeführt werden. Bei mehrtägigen Tests sollte jeden Morgen ein kurzes Gespräch zwischen den Prüfern und dem beteiligten technischen Personal des Auftraggebers stattfinden, in dem geklärt wird, was geplant ist. Nach Abschluss der Arbeiten sollte eine kurze Zusammenfassung erfolgen.

Anfangsgespräch

Am ersten Tag sollte ein kurzes Begrüßungsgespräch mit dem Auftraggeber und dem beteiligten technischen Personal stattfinden. Es empfiehlt sich, noch einmal das Prüfobjekt und das Prüfbedingungen zu besprechen, um sicherzustellen, dass alle Beteiligten die gleichen Vorstellungen vom Prüfobjekt und Umfang der Tests besitzen. Eventuelle Missverständnisse können hier noch einmal aus dem Weg geräumt werden.

Auch bei einem IS-Penetrationstest über das Internet sollte eine Vorabstimmung durchgeführt werden.

Prüfbedingungen

Danach werden die Prüfbedingungen für den Test in Augenschein genommen. Die Prüfer klären im Beisein der Ansprechpartner des Auftraggebers ab, ob die besprochenen Voraussetzungen für den Test erfüllt sind. Anschließend testen die Prüfer, ob der Zugang zu den IT-Systemen wie abgesprochen möglich ist und stellen fest, ob die Ansprechpartner auskunftsfähig sind.

Praktische Prüfung

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

Die Aufteilung in die Module wurde vorgenommen, um Außenstehenden einen Überblick über die getetesten Aspekte zu vermitteln. Die Reihenfolge der Module kann individuell festgelegt werden, auch können einzelne Module mehrfach durchgeführt oder gleichzeitig abgearbeitet werden. Dies geschieht beispielsweise, wenn in einem Modul die Ergebnisse für einen Teiltest eines anderen Moduls geliefert werden. Teilweise hängt die Reihenfolge auch von der Verfügbarkeit weiterer technischer Ansprechpartner ab.

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

Modul 1 – konzeptionelle Schwächen

Meistens werden den Prüfern bei der Sichtung der Unterlagen über das Prüfobjekt in der Vorbereitungszeit offene Punkte und Fragen auffallen. Diese können auf konzeptionelle Schwächen des Prüfobjekts hinweisen, die den Verantwortlichen vor Ort vielleicht nicht aufgefallen sind. Beispielsweise könnte eine Institution so aufgebaut sein, dass für jede Fachanwendung voneinander unabhängige Mitarbeiter eingesetzt werden. Die IT-Administratoren haben dann teilweise ohne Kenntnis des Schutzbedarfs der Fachanwendung die Aufgabe, diese mit wenig Geld und Personal zu hosten und zur Verfügung zu stellen. Die einzelnen IT-Anwendungen können dann jede für sich sicher konzipiert sein. Wenn sie aber beispielsweise alle auf einem IT-System gehostet sind, dann können, selbst wenn das IT-System selbst wieder sicher aufgebaut wird, Schwachpunkte durch die unterschiedlichen Rechte der IT-Anwendungen entstehen.

Die Prüfer können solche Fragen durch praktische Tests, teilweise aber auch durch Gespräche mit den Verantwortlichen klären.

Modul 2 – Umsetzung Härtungsmaßnahmen

In diesem Modul wird festgestellt, ob die für das Prüfobjekt erforderlichen Härtungsmaßnahmen umgesetzt sind. Hierbei sollten mindestens folgende Punkte geklärt werden:

- offene Ports
- Schnittstellen
- Aktualität der Patchstände und der eingesetzten Softwareversionen
- Zugangsvoraussetzungen zu Programmen / Authentisierung
- Absicherung der Dienste / Regelwerke

Je nach IT-Anwendung kommen weitere individuelle Punkte hinzu, die aus den Dokumentationen der IT-Anwendung selbst erarbeitet werden sollten.

Offene Ports

Mit einem Portscan können die IT-Systeme, auf denen die IT-Anwendung läuft, auf offene Ports geprüft werden. Erwartet wird, dass nur für die IT-Anwendung benötigte Ports erreichbar sind. Werden weitere Dienste (beispielsweise aus einer Standardinstallation der IT-Systeme) gefunden, so wird empfohlen, diese nach Abschluss der Tests abzuschalten.

Schnittstellen

Werden auf einem IT-System mehrere Dienste gehostet, entstehen möglicherweise unerwünschte Schnittstellen zu der zu testenden IT-Anwendung. Die Administratoren und Fachverantwortlichen sollten den Einsatzzweck der gefundenen Schnittstellen genau erläutern können.

Patchstände und eingesetzte Softwareversionen

Es wird überprüft, welche Softwareversionen mit welchen Patchständen im Einsatz sind. Da in den neuesten Versionen meist die aktuell bekannten Schwachstellen beseitigt sind, ist es ratsam, die aktuellen Versionen einzusetzen. In einigen Fällen ist das aus Kompatibilitätsgründen zu anderen abhängigen IT-Anwendungen nicht per regulärem Update-Mechanismus möglich. In diesem Fall sollte der Administrator die aktuellen Patches per Hand eingespielt haben. Auch dies ist (je nach IT-Abhängigkeiten) nicht immer möglich. Dann muss aufgezeigt werden, welche alternativen Schutzvorkehrungen getroffen wurden, um die aktuell bekannten Schwachstellen einzudämmen.

Zugangsvoraussetzungen Programme/Authentisierung

Hier werden die Zugangsvoraussetzungen zu den verschiedenen IT-Systemen und Programmen des Prüfobjektes geprüft. Es sollten u.a. folgende Fragen geklärt werden: Wer hat Zugriff auf die IT-Anwendungen bzw. das IT-System? Wie sind die Zugangsvoraussetzungen und die Authentisierung geregelt? Wie werden Authentisierungsmittel (Token, Passwörter) geschützt? Sind über das Netz auch unberechtigte Personen angebunden? Werden Passwörter verlangt? Sind hierbei Standardpasswörter gesetzt?

Absicherung der Dienste / Regelwerke

Zuletzt müssen noch die weiteren Absicherungen des Prüfobjekts selbst getestet werden. Wenn es sich beispielsweise um eine Firewall handelt, so sollte das Regelwerk auf Schwachpunkte untersucht werden. Es könnte beispielsweise eine temporär angelegte Regel noch aktiv sein. Bei anderen Diensten kann die Konfigurationsdatei geprüft werden oder auf indirektem Weg getestet werden, ob Funktionen verfügbar sind, die abgeschaltet sein sollten. Beispielsweise sollten bei einem Webserver nur die benötigten HTTP-Optionen freigeschaltet sein. Durch die Abfrage der Optionen kann ein Prüfer herausfinden, ob dies tatsächlich der Fall ist, ohne in die Konfigurationsdatei zu schauen.

Modul 3 – Bekannte Schwachstellen

Bei diesem Modul wird das Prüfobjekt auf bekannte Schwachstellen untersucht. Dies kann aufgrund der in Modul 2 vorgefundenen Patchstände geschehen oder unter Einbeziehung von sogenannten Schwachstellenscannern durchgeführt werden. Das sind Tools, die Versionen und Patchstände der eingesetzten Betriebssysteme und Applikationen abfragen. Die Ergebnisse dieser Tools können ungenau sein, weil bei den nicht invasiven Scannern lediglich die Banner der IT-Anwendungen abgefragt werden. Ein versierter Administrator kann diese fälschen und somit einen falschen Stand vortäuschen. Der Einsatz von Schwachstellenscannern lohnt sich, wenn in kurzer Zeit eine große Menge von IT-Systemen überprüft werden soll. Ein invasiver Scanner

probiert zusätzlich aus, ob potentielle Schwachstellen über Exploits ausgenutzt werden können. Dies kann in Modul 4 durchgeführt werden, um Gewissheit über die Ausnutzbarkeit von Schwachstellen zu erlangen.

Optional: Modul 4 – Exploits

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

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

Abschlussgespräch

Nach Abschluss der Tests sollte ein Gespräch zwischen den Prüfern und den Ansprechpartnern seitens der Auftraggeber stattfinden. Ziel ist, über den Verlauf und die Ergebnisse der praktischen Prüfung zu informieren. Es sollte beim Vorgespräch festgelegt werden, welche Personen der Institution anwesend sein werden, damit die Prüfer die Inhalte des Gesprächs entsprechend des Zielpublikums aufarbeiten können. Wenn eine Medienunterstützung (z.B. Beamer) benötigt wird, so sollte auch das frühzeitig geklärt werden, damit zum Gespräch alles verfügbar ist.

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

> Um die Tests nicht unnötig zeitlich auszudehnen, wird *vom BSI empfohlen*, nicht alle Auswertungen vor Ort vorzunehmen. Daher kann die weitere Vorstellung der Schwachstellen im Abschlussgespräch unter Umständen nur unter Vorbehalt stattfinden. Eine verbindliche Darstellung aller gefundenen Schwachstellen sollte im Bericht zu finden sein.

4.1.3 Bericht

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

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

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

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

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

Für die Bewertung der Schwachstellen können verbreitete Industriestandards wie CVSSv2 [8] oder DREAD [9] von Microsoft herangezogen werden.

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

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

Schadenspotenzial	Erforderliche Reaktion	Erläuterung
hoch	sofort	Fremdsteuerung des Prüfobjekts durch Angreifer möglich, Verlust von sensiblen Daten möglich, Veränderung des Prüfobjekts oder Auslesen von sensiblen Daten durch Angreifer möglich
mittel	kurzfristig	Schwachstellen, die schwerwiegende Angriffe ermöglichen können
niedrig	mittelfristig	Schwachstellen, die ein unbestimmtes Angriffspotenzial haben
zur Information	langfristig	Verbesserungspotenzial

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

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

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

Es wird empfohlen, eine Schwachstellenbeschreibung einmal vorzunehmen, hierzu ein Beispiel genau auszuführen und darauf hinzuweisen, dass alle gleich aufgebauten IT-Systeme, ebenfalls diesbezüglich gepatched werden müssen. Wenn bei der praktischen Prüfung jeder Systemtyp stichprobenartig nur einmal getestet wird, kann der Kosten- und Zeitaufwand des IS-Penetrationstests zusätzlich gering gehalten werden.

5 Anhang:

5.1 Checklisten

5.1.1 Hilfestellung für die Beauftragung von IS-Penetrationstests

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

Vorgabe	**Spezifizierung**	**Bemerkung Institution (erledigt oder nicht relevant, weil...)**
Motivation für IS-Penetrationstest (Kapitel 2.1.1)	Check der Sicherheitsmaßnahmen, Verdacht auf Angriff, entdeckter Angriff	
Anforderung an Prüfer (Kapitel 2.2)	Fachliche Anforderungen	
	Weitere Fähigkeiten	
	Arbeitet für Prüfstelle	
	Technische Qualifikation / Zertifikate	
Rahmenbedingungen (Kapitel 2.3)	Vertrag, NDA, Speicherzeit von Daten	
	Datenschutz, Geheimschutz, Personalvertretung	
	Sonstiges (Wartungsarbeiten)	
Festlegung des Prüfobjekts zwischen Prüfer und Institution (Kapitel 3.1.1)	Beispielsweise Netzkoppelelemente (Router, Switches, Gateways), Sicherheitsgateways (Firewall, Paketfilter, Intrusion Detection System, Virenscanner etc.), Server (Datenbankserver, Webserver, Fileserver, Speichersysteme etc.), Telekommunikationsanlagen, Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop), Clients, Drahtlose Netze (WLAN , Bluetooth etc.), Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)	
Festlegung des Prüfumfangs (Kapitel 3.1.2)	Prüftiefe	
	Prüfort	

Vorgabe	Spezifizierung	Bemerkung Institution (erledigt oder nicht relevant, weil...)
	Prüfzeitraum	
	Prüfbedingungen	
Verantwortlichkeiten (Kapitel 3.1.3)	Projektverantwortliche bei Prüfern und Institution	
Meilensteinplan (Vgl. auch Mindestanforderungen IS-Penetrationstest Kapitel 5.1.2)	Einarbeitungsphase	
	Testphase	
	Berichtsphase	

5.1.2 Rahmenbedingungen und wiederkehrende Elemente bei einen IS-Penetrationstest

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

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

Arbeitspaket	Unterpaket 1	Unterpaket 2	Unterpaket 3	Erforderliche Personen	Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)
Einarbeitung Prüfer (Kapitel 4.1.1)	Dokumente sichten			Prüfer	
Vorbereitung Institution	Prüfumgebung bereitstellen (Kapitel 3.1.2 - Prüfbedingungen)			Institution/Hoster (Administrator, Techniker)	
	Kunden/Mitarbeiter informieren (Kapitel 2.3)			Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
	Datenschutzbeauftragten/Personalrat/Geheimschutzbeauftragten einbeziehen (Kapitel 2.3)			Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	

Arbeitspaket	Unterpaket 1	Unterpaket 2	Unterpaket 3	Erforderliche Personen	Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)
	Dokumente an Prüfer schicken (Kapitel 4.1.1)			Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
Test des Prüfobjekts (Kapitel 4.1.2)	Anfangsgespräch			Prüfer, Institution/Hoster (IT-Sicherheitsverantwortlicher, Fachverantwortliche, Administratoren)	
	Prüfumgebung			Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
	Praktische Prüfung	Modul 1 – konzeptionelle Schwächen		Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
		Modul 2 – Umsetzung Härtungsmaßnahmen	offene Ports	Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
			unnötige Schnittstellen	Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
			Patchstände und eingesetzte Softwareversionen	Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverantwortlicher oder Fachverantwortliche)	
			Zugangsvoraussetzungen Programme, Authentisierung	Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverant	

Arbeitspaket	**Unterpaket 1**	**Unterpaket 2**	**Unterpaket 3**	**Erforderliche Personen**	**Bemerkung der Prüfer (beispielsweise erledigt oder nicht durchgeführt, weil...)**
				wortlicher oder Fachverantwortliche)	
			Absicherung der Dienste / Regelwerke	Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverant wortlicher oder Fachverantwortliche)	
		Modul 3 – Bekannte Schwachstellen		Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverant wortlicher oder Fachverantwortliche)	
		Optional: Modul 4 – Exploits		Prüfer, Ansprechpartner der Institution/Hoster (IT-Sicherheitsverant wortlicher oder Fachverantwortliche)	
	Abschlussgespräch			Prüfer, Institution/Hoster (IT-Sicherheitsverant wortlicher und Fachverantwortliche)	
Bericht (Kapitel 4.1.3)		Einleitung		Prüfer	
		Managementzusammenfassung			
		Technische Beschreibung der Schwachstellen mit Empfehlungen und Einstufung der Kritikalität			

5.2 Ablaufplan

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

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

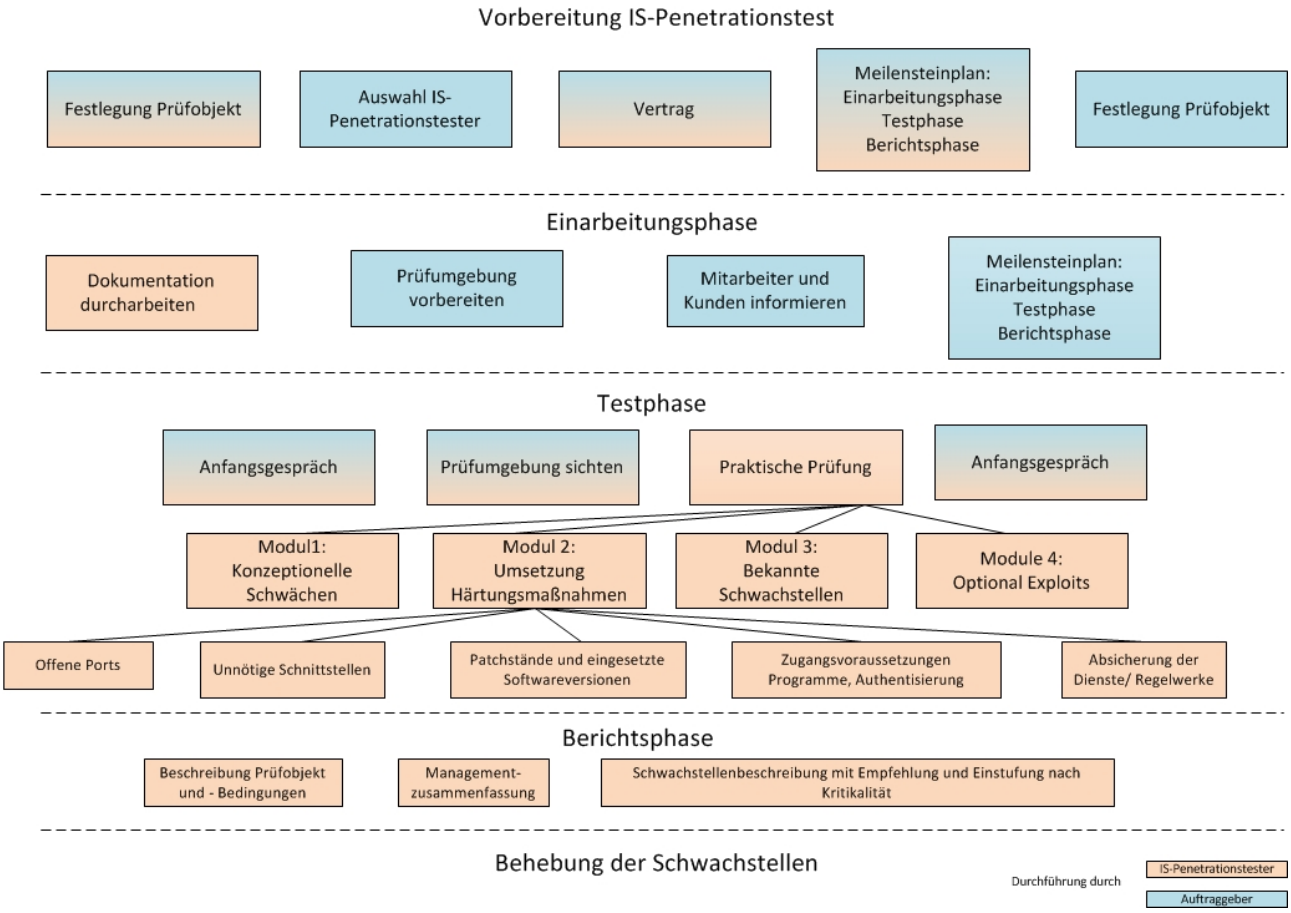


Abbildung 3 Ablauf eines IS-Penetrationstest

6 Glossar

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

Begriff	**Erläuterung**
APT	Ein Advanced Persistent Threat (APT) ist ein sehr komplexer, zielgerichtet durchgeführter Cyber-Angriff
Buffer Overflow	Es werden Daten in einen Speicherbereich geschrieben, der kleiner als die geschriebene Datenmenge ist. Wenn das Programm dies nicht abfängt, wird der Speicher hinter dem reservierten Speicherbereich überschrieben. Bei Kenntnis der Nutzung des Speicherinhalts können hierdurch gezielte Angriffe durchgeführt werden.
DoS	Bei einem Denial of Service (DoS)-Angriff werden so viele Anfragen an einen Dienst gleichzeitig ausgeführt, dass er (kurzfristig) ausfällt. Wenn die Anfragen von verschiedenen IP-Adressen ausgeführt werden, so wird auch von einem distributed Denial of Service (dDoS) gesprochen.
Exploit	Ein Exploit ist ein Programm, das eigens zum Ausnutzen einer Sicherheitslücke geschrieben wurde.
IS-Penetrationstest	Bei IS-Penetrationstests werden vorrangig Schnittstellen nach außen untersucht, über die potenzielle Angreifer in die untersuchten IT-Systeme eindringen könnten. Hierbei werden Konfigurationsfehler sowie noch nicht behobene Schwachstellen identifiziert.
IS-Revision	Die IS-Revision zielt darauf ab, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und der Sicherheitsprozesse zu optimieren.
IS-Webcheck	Mit einem IS-Webcheck des BSI wird der Sicherheitsstand einer Internetpräsenz geprüft.

Begriff	Erläuterung
	Hierbei werden Tests auf die Webanwendung größtenteils durch den Einsatz automatisierter Methoden über das Internet durchgeführt.
Nicht invasiver Schwachstellenscan	Ein Prüfer scannt mit eigenen Geräten im Zielnetz nach bekannten Schwachstellen. Er setzt hierzu Schwachstellen- scanner ein, nutzt die Schwachstellen aber nicht aus.
Portscan	Ein Prüfer scannt in einem Netzwerk oder Netzsegment nach offenen Ports.
Prüfumfang	Der Prüfumfang definiert die Prüftiefe (technisches Sicherheitsaudit, nicht invasiver Schwachstellenscan oder Einsetzen von Exploits), den Prüfort (Institution Rechenzentrum, Institution Büroräume oder vom Prüflab aus übers Internet), den Prüfzeitraum und die Einrichtung der Prüfumgebung (Freischaltung von MAC-Adressen für Laptops von Prüfern, Freischalten des Sicherheitsgateways für die Prüfer).
Prüfobjekt	Das Prüfobjekt grenzt ab, welches IT-System getestet wird. Hierbei wird aus Angreifersicht geschaut, wo Schnittstellen auf die IT-Systeme sind, über die ein Angreifer eindringen kann. Übliche Prüfobjekte sind u.a. • Netzkoppelelemente (Router, Switches, Gateways) • Sicherheitsgateways (Firewalls, Paketfilter, Intrusion Detection System, Virenscanner etc.) • Server (Datenbankserver, Webserver, Fileserver, Speichersysteme etc.) • Telekommunikationsanlagen • Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop) • Clients • Drahtlose Netze (WLAN , Bluetooth) • Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)

Begriff	Erläuterung
Prüftiefe	Es wird festgelegt, in welcher Tiefe ein Test durchgeführt werden soll. Hierbei kann beispielsweise ein Sichereitsaudit, ein nicht invasiver Schwachstellenscan oder das Einsetzen von Exploits (aktiver Schwachstellenscan) zur Auswahl stehen.
Social Engineering	Bei Social Engineering Angriffen werden über die Gutgläubigkeit der Mitarbeiter/Zielpersonen, aber auch über Informationen, die im Internet (beispielsweise Social Media oder Foren) frei verfügbar sind, Kenntnisse über die Strukturen einer Institution und auch über deren IT-Systeme zusammengetragen, um bei weiteren Angriffen gezielt darauf aufbauen zu können.
Spoofing	Spoofing steht für das Vortäuschen einer falschen Identität. Beispielsweise können die MAC-Adresse, die IP-Adresse oder die Absenderadresse bei E-Mails relativ leicht gefälscht werden. Wird dies gemacht, wird von Spoofing-Angriffen gesprochen.
Technisches Sicherheitsaudit	Bei einem technischen Sicherheitsaudit wird anhand der Versionen der eingesetzten IT-Anwendungen auf mögliche Schwachstellen geschlossen. Die Prüfer bedienen die IT-Systeme hierbei nicht selbst, sondern lassen sich von einem Administrator zeigen, welche Versionen eingesetzt und welche Härtungsmaßnahmen durchgeführt wurden.

7 Referenzen

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

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

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

[3] IS-Webcheck
https://www.bsi.bund.de/dok/6621966

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

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

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

[7] IS-Webcheck

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

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

https://www.first.org/cvss

[9] Microsoft Thread Modeling (Einstufung mit DREAD)

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