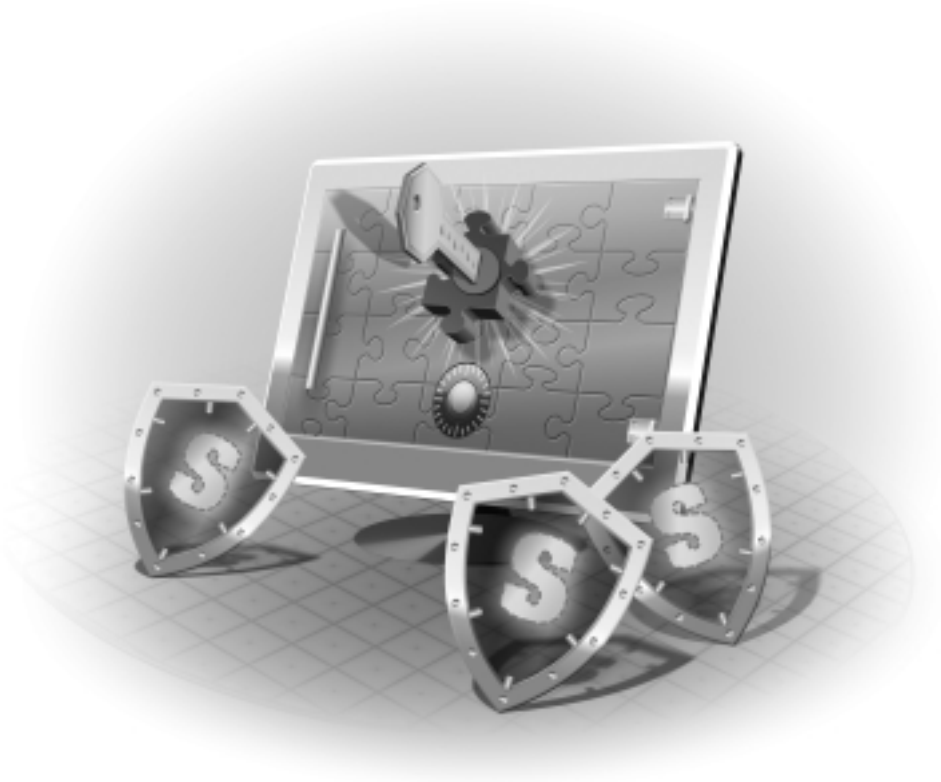
Computer & Literatur Verlag GmbH

Penetrations-Tests

von Thomas Werth



Bibliographische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2012

Zavelsteiner Straße 20, 71034 Böblingen
E-Mail: info@cul.de
WWW: http://www.CuL.de

Coverdesign: Hawa & Nöh, Neu-Eichenberg
Satz: C&L Verlag
Fotografien in Kapitel 3: Nadine Werth
Druck: PUT i RB DROGOWIEC
Printed in Poland

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt

ISBN 978-3-936546-70-5

Gewidmet meiner lieben Familie:

Meiner wunderbaren Frau Nadine,
meiner phantastischen Tochter Maya
und unserem Neuzugang Tom

Inhalt

LITERATUR

JÖRG BRAUN: Das VirtualBox-Buch. Hosts und Gäste. C&L Verlag 2012. 450 Seiten, ISBN 978-3936546-71-2

JÜRGEN DANKOWEIT (Hrsg.): FreeBSD. Installieren, Konfigurieren, Vernetzen. C&L Verlag 2009. 751 Seiten, ISBN 978-3936546-41-5.

RED. FREEX (Hrsg.): Linux im Netz. Dienste auf Server, Desktop, Notebook. C&L Verlag 2006. 864 Seiten, ISBN 978-3936546-34-7

DR. ROLF FREITAG: Die Kunst des Verdeckens. Daten verschleiern, verschlüsseln, zerstören. C&L Verlag 2011. 366 Seiten, ISBN 978-3936546-65-1

DR. MATTHIAS LEU: Check Point NGX. Das Standardwerk für FireWall-1/VPN-1. C&L Verlag 2007, 1292 Seiten, ISBN 978-3936546-37-8

ROSA RIEBL: Mozilla. Firefox, Thunderbird, SeaMonkey. C&L Verlag 2010. 446 Seiten, ISBN 978-3936546-52-1

MARC RUEF: Die Kunst des Penetration Testing. Handbuch für professionelle Hacker. C&L Verlag 2007. 911 Seiten, ISBN 978-3936546-49-1

FABIAN THORNS (Hrsg.): Das Virtualisierungs-Buch. Konzepte, Techniken und Lösungen. 2. aktual. Aufl., C&L Verlag 2008, 799 Seiten, ISBN 978-3936546-56-9
(im Verlag vergriffen)

THOMAS WERTH: Die Kunst der digitalen Verteidigung. Sicherheitsstrategien, Software-Diagnosen, Forensische Analysen. C&L Verlag 2009. 607 Seiten, ISBN 978-3936546-59-0

Geleitwort

Die Informationssicherheit und ihre Überprüfung war schon immer eminent wichtig, die Form der Informationen spielte dabei eigentlich noch nie eine Rolle. Egal, ob sie vor ein paar Jahrzehnten nur auf Papier geschrieben waren oder heute überwiegend auf einem digitalen Datenträger gespeichert sind – schützenswerte Daten wurden schon immer unzugänglich aufbewahrt und die Wirksamkeit des Schutzes wurde schon immer regelmäßig und umfassend kontrolliert.

Wirklich verändert hat sich in den letzten Jahren die Bedrohungslage, der sich Unternehmen ausgesetzt sehen. Während einst noch Daten von Servern illegal kopiert wurden, um daraus einen wirtschaftlichen Vorteil zu erhalten, so wird damit heute massiver und vor allem öffentlicher umgegangen. Kundenlisten tauchen im Internet auf, Server werden kompromittiert und ganzen Internetseiten werden für Stunden lahmgelegt. Die Folgen solcher Angriffe können enorm sein, sie reichen vom gerade noch verschmerzbaren Imageschaden bis hin zum Verlust der Existenzgrundlage.

Eine wirkungsvolle Strategie für die Datensicherheit von Unternehmen muß deshalb aus mehreren Komponenten bestehen, Compliance, Risikomanagement, Informationssicherheit, Krisenmanagement, Know-how-Schutz, Zutrittskontrolle, Awareness und Datenschutz sind unabdingbar. Sind diese Punkte alle gemäß den internen Richtlinien vollständig oder zumindest in Teilbereichen umgesetzt, kommt der Teil der Sicherheitsstrategie, der von vielen Unternehmen vergessen oder verdrängt wird: die professionelle Überprüfung der vorhandenen Sicherheit von Daten, Informationen und Netzwerken. Gegen Fehler ist selbst der gewissenhafteste und erfahrenste Administrator nicht gefeit; ihm kann bei der Konfiguration einer Firewall und ihrer Integration in das Netzwerk ein kleiner Fehler unterlaufen, der sich auf die Sicherheit des gesamten Unternehmens auswirkt. Damit er nicht auf Dauer unbemerkt bleibt und unabsehbare Folgen nach sich ziehen kann, müssen die Systeme regelmäßig überprüft werden.

In den Medien werden Angreifer oft als frühreife Jugendliche gezeigt, die Skimasken tragen, neben der Tastatur die Chipstüte liegen haben und die gewonnen Daten illegal weiterveräußern oder veröffentlichen. Ja, natürlich gibt es die, aber es gibt auch die professionellen Angreifer, die Auftragsarbeiten durchführen. Oder die Geheimdienste, die im Interesse der

eigenen Wirtschaft Unternehmen anderer Länder ausspionieren. Technisch versierte Angreifer können von außen und von innen kommen und sind oft sehr gut geschützt gegen Verfolgung, weil sie es verstehen, ihre Spuren zu verwischen. Von diversen, im Internet dokumentierten Angriffen und den Warnungen der Landesämter für Verfassungsschutz wissen wir, daß insbesondere das Know-how deutscher Unternehmen gern zum Ziel von Angreifern wird. Viele dieser Angriffe werden leider zu spät entdeckt, nämlich erst dann, wenn der Schaden schon eingetreten ist. Allerdings darf nicht vergessen werden, daß die Folgen nicht nur für das betroffene Unternehmen gravierend sein können, sondern die Angriffe auf die deutschen Wirtschaftsunternehmen und der resultierende Abfluß von Know-how zur Schwächung der Gesamtwirtschaft beitragen.

Mir ist natürlich klar, daß es den Unternehmern häufig nicht leicht fällt, zwischen Produktivität und ihrem Schutz den richtigen Mittelweg zu finden. Aber diese beiden Punkte müssen ineinander greifen und gegenseitig voneinander profitieren! Weil die aktive Unterstützung der Informationssicherheit nun mal einer der Grundpfeiler der Wirtschaftsleistung ist, muß sie ihren festen Platz in der Unternehmenskultur haben.

Um sein eigenes Unternehmen auf der Informations- und Datenebene zu schützen und diesen Schutz zu überprüfen, muß man so vorgehen, arbeiten und denken wie ein professioneller Angreifer. Der Autor dieses Buches gibt Ihnen als Leser das Werkzeug an die Hand, um genau das tun zu können: Das Netzwerk und die Datensicherheit des Unternehmens so zu überprüfen, wie ein Angreifer versuchen würde, in ein Unternehmen einzudringen.

Professionelle Angriffe auf Unternehmen sind gut organisiert und wohldurchdacht. Sie sind glücklicherweise nicht immer von Erfolg gekrönt, aber leider noch immer ausreichend oft. Die Unternehmer und die Administratoren müssen sich deshalb Gedanken darüber machen, wie sie die Sicherheit des Unternehmens und damit die Unternehmenswerte erhalten können. Sie kann maßgeblich davon abhängen, wie sicher die Infrastruktur für die Daten ist und wie leicht ein Angreifer sich Zugriff verschaffen kann, ohne dabei bemerkt zu werden. Die technischen Aspekte von Sicherheitsüberprüfungen sowie die konzeptionellen Ansätze für eine professionelle Vorgehensweise finden sich in diesem Werk wieder. Der Leser bekommt eine vollständige Übersicht darüber, wie Dienste und Programme angegriffen werden und hat die Möglichkeit, die Vorgehensweisen selbst im Unternehmen zum eigenen Schutz zu testen. Die unterschiedlichen Angriffsmethoden auf Unternehmensnetzwerke werden ebenso ausführlich vorgestellt wie die benötigten Hilfsmittel und Werkzeuge. Weil die Komplexität von Angriffen gestiegen ist, ist auch die Komplexität von professionellen Sicherheitsüberprüfungen gestiegen. Sie und die enormen Anforderungen kann der Leser nach der Lektüre dieses Werks meistern und seinem Unternehmen zu einem hohen Maß an Sicherheit verhelfen.

Marko Rogge, IT-Sicherheitsberater und IT-Forensiker

Es gibt Momente im Leben, die auch in der Wiederholung nichts von ihrem Zauber verlieren.

— Tom —

Liebe Leser,

eine hundertprozentige Systemsicherheit kann es nur dann geben, wenn der Computer nicht mit einem Netzwerk verbunden ist und keine Laufwerke besitzt, über die Schadsoftware auf ihn gelangen kann. Dies wird aber in einem Unternehmen niemals der Fall sein, dort kommunizieren die Arbeitsplatz-PCs mit den Dateiservern, Finanz- und Buchhaltungsdaten müssen an die DATEV und die Staatskassen übertragen werden, die Kunden und Lieferanten können ihre Bestellungen und Bestände über einen HTTP-Zugriff aufgeben und einsehen und die Mitarbeiter möchten in ihrer Mittagspause im Internet surfen. Damit es nicht zu einem illegalen Datenabfluß kommen kann, besteht sogar eine gesetzliche Pflicht zur Sicherung der Computersysteme und Netzwerke. Nur: Wer weiß denn, wie sicher sie trotz aller Maßnahmen wie Authentifizierung, Firewalls, DMZ und Filter wirklich sind? Die tatsächliche Sicherheit kann nur dann festgestellt werden, wenn die Systeme einem Einbruch – Penetrations-Test – unterzogen werden, die Guten quasi schneller sind als die Bösen. Sind die Einbrüche erfolgreich und führen zu einem Datenabfluß, erfährt man automatisch, wo noch Sicherheitslücken vorliegen und wie sie geschlossen werden müssen.
Penetrations-Tests sind also systematische Einbrüche in Computer und Netzwerke, um den Grad der vorhandenen Sicherheit zu überprüfen und zu bewerten. Der Leitgedanke der Systematik hat mich auch beim Schreiben dieses Buchs begleitet. Mein Ziel war ein generisches Nachschlagewerk, in dem alle Verfahren beschrieben sind, um ein bestimmtes Testziel zu erreichen. Weil es wenig sinnvoll ist, den Kompletteinbruch in eine Firma X zu beschreiben, habe ich die Tests in Angriffe auf einzelne Dienste, Programme und Netzwerke aufgedröselt. Dabei habe ich die Ziele jedes Angriffs einzeln aufgeschlüsselt und die verschiedenen Verfahren beschrieben, wie ein Penetrations-Tester Zugriff auf das jeweilige

System und seine Daten erlangt. Mit diesen Anleitungen ist man dann auch in der Lage, einen Angriff auszuführen, in dem mehrere Ziele kombiniert werden.
Ich richte mich bei den Tests nach der Methodik des Open Source Security Testing Methodology Manual (OSSTMM). Nach meinen Erfahrungen ist es das einzige Handbuch, das alle Bereiche von Penetrations-Tests abdeckt und würdige es im Buch entsprechend.
Als Arbeitsumgebung nutze ich die spezielle Linux-Distribution Backtrack und diverse Programme und Frameworks wie beispielsweise Metasploit. Wenn Sie ein anderes System bevorzugen, können Sie dies natürlich entsprechend erweitern, ich biete Ihnen alle Informationen dazu.

Zum Schluß möchte mich noch bedanken:
Zuerst meiner Frau Nadine für ihre Geduld und ihr Verständnis, insbesondere wenn ich mal wieder mehr mit dem Computer als mit ihr verheiratet war. Ich freue mich schon wieder auf die Zeit, wenn sie nicht mehr ohne mich den Kindern aus meinen herumliegenden Hacker-Büchern vorlesen muß. Womit ich auch meine zwei Kindern Maya und Tom dafür danke, daß sie mir jeden Tag ein Lächeln ins Gesicht zaubern. Ebenso danke ich meinen Eltern, Schwiegereltern und meiner großen Familie. Dabei möchte ich Jenny B. an dieser Stelle besonders hervorheben, die eine wunderbare Patentante ist. Ebenso verdient auch Sven K. eine besondere Erwähnung. Marko Rogge bin ich für die inzwischen mehrjährige Unterstützung mehr als dankbar und hoffe, daß dies in der Zukunft so bleiben wird. Auch meine lieben Freunde und Kollegen möchte ich nicht vergessen, ohne die das Leben doch um einiges ärmer wäre. Ebenso möchte ich Volker danken, weil er mich immer noch ohne zu zögern unterstützt, wenn ich mal Hilfe brauche. Vielen Dank auch an Steffi G., die sich als Fotomodell für die Bilder in Kapitel 3 zur Verfügung gestellt hat. Dank auch an meine Lektorin und Verlegerin Frau Riebl, die auf ihre gewohnt charmante Art das bestmögliche Werk aus einem Autor herauskitzelt.

Ihr

Thomas Werth

Kapitel 1
Die Testorganisation

Ein Penetrations-Test ist ein auftragsgesteuerter Einbruch in die datenverarbeitenden Systeme eines Unternehmens, der zum Ziel hat, den Sicherheitszustand der Systeme festzustellen. Gelingt dem Tester der Einbruch und kann er Zugriff auf vertrauliche Informationen erlangen, beispielsweise in einer bestehenden Verbindung zwischen mehreren Computern Paßwörter mitschneiden, Daten aus Dateien oder Datenbanken auslesen oder ihren Informationsgehalt manipulieren, ist dies der Beweis, daß das System Sicherheitslücken hat. Der Auftraggeber muß sich dann darum kümmern, diese Sicherheitslücken zu schließen. Gelingt es dem Tester jedoch nicht, in die Systeme einzudringen, kann davon ausgegangen werden, daß die Systeme zu diesem Zeitpunkt als sicher erachtet werden können. »Zu diesem Zeitpunkt« deswegen, weil es durchaus der Fall sein kann, daß ein paar Tage nach dem erfolglosen Penetrations-Test eine generelle Sicherheitslücke in einem Programm oder in einer Verbindung entdeckt wird, auf deren Grundlage eine Angriffsmethode entwickelt wird, mit der ein Unbefugter in das System eindringen kann.

Die Methoden, wie in ein datenverarbeitendes System eingebrochen werden kann, sind nicht unbedingt nur technischer Natur. Natürlich gibt es etliche auf einen Einbruch spezialisierte Werkzeuge beziehungsweise können an sich harmlose Programme zweckentfremdet werden, um in eine Anlage einzudringen. Ein Einbruch kann aber nur dann gelingen, wenn der Penetrations-Tester vorher hinreichend Informationen über die Systeme besitzt. Dazu gehören die Namen von Computern und ihre Adressen, über die sie in einem Netzwerk erreichbar sind. Sowie die Art der auf den Computern angebotenen Programme und die Zugangsdaten, über die sich die Benutzer an den Systemen authentifizieren müssen. Diese Informationen müssen primär mit technischen Mitteln gesammelt werden, denn ein Programm kann nun mal schneller rechnen als sein Anwender und langweilt sich nicht beim schier endlosen Abarbeiten von Tabellen. Manchmal gelingt es aber einfach nicht, die wichtigen Informationen mit einem Computer zu ermitteln oder auf gut Glück ein System zu penetrieren. In solchen Fällen muß der Tester die Mitarbeiter, die an den Computern arbei-

ten, in seine Recherchen einbeziehen. Sie kennen ja mindestens die eigenen Zugangsdaten und das eine oder andere Detail zu den Systemen. Damit die Anwender einen Fremden – der der Penetrations-Tester ja ist – großzügig mit Informationen versorgen, muß er sich Mitteln bedienen, die eigentlich unterhalb einer moralischen Gürtellinie angesiedelt sind. Quasi als Nebeneffekt erforscht er dabei die Verschwiegenheit des Personals in einem Unternehmen. Schließlich macht der Penetrations-Tester nichts anderes als ein Unbefugter, der Geschäftsgeheimnisse erlangen möchte: Leute aushören und sie dazu bringen, in einer bestimmten Weise zu handeln.

1.1 DER AUFTRAG

Ein Penetrations-Test bedarf einer methodischen Vorgehensweise, schließlich geht es um die Feststellung des Sicherheitszustands eines ganzen Unternehmens. Würde hier unkoordiniert und unstrukturiert vorgegangen, wären die erzielten Ergebnisse zufällig, wären nicht nachvollziehbar und deswegen ungültig.
Nachfolgend werden die formalen Anforderungen an Penetrations-Tests vorgestellt.

1.1.1 Testtypen

Man könnte meinen, daß der einzige Sicherheitstest für ein Computersystem der Penetrations-Test ist. Dieser Begriff hat sich in den Medien durchgesetzt und scheint sich inzwischen als Oberbegriff für alle Sicherheitstests durchgesetzt zu haben. Es gibt aber mehrere Ausprägungen von Sicherheitsüberprüfungen.

Regelkonformität (Compliance Test)

Die Organisation eines Unternehmens bewegt sich nicht in einem rechtsfreien Raum. Vielmehr geben zahlreiche Gesetze und Vorschriften vor, wie Geschäftsvorfälle zu dokumentieren sind, was wie lange in einem Archiv gelagert werden muß und wie die datenverarbeitenden Systeme beschaffen sein müssen.
In erster Linie gibt das Handelsgesetz vor, daß die Computersysteme einbruchssicher sein müssen, so daß keine Betriebsgeheimnisse abfließen und in die Hände Unbefugter gelangen können, um Schaden von der Firma und der wirtschaftlichen Wettbewerbsfähigkeit des ganzen Staatsgebildes abzuwehren. Zur Konkretisierung dieser gesetzlichen Forderung wurden zahlreiche Standards und weitere Gesetze entwickelt, die bestimmte technische und organisatorische Maßnahmen vorschlagen. Allerdings steht es den Unternehmen frei, selbst interne Sicherheitsrichtlinien aufzustellen, die von den einzelnen Fachabteilungen eingehalten werden müssen. Natürlich müssen sich diese an den gesetzlichen Vorschriften orientieren.
Weil die Umsetzung von Normen und Standards mit viel Arbeit verbunden ist und zu Unbequemlichkeiten bei manchen Arbeitsabläufen führen kann, ist es mehr oder weniger gang und gäbe, daß sich im Laufe der Zeit Laxheiten bei ihrer Einhaltung einschleifen. Dies kann so weit führen, daß die Systeme unsicher werden und sogar gegen die geltenden Gesetze verstoßen wird.

Die Geschäftsleitung tut also gut daran, ab und zu nachzuforschen, ob im Tagesgeschäft die einstmals als bindend verabschiedeten Richtlinien auch wirklich (noch) angewandt werden. Eine Prüfung auf Einhaltung der Regeln heißt Compliance Test. Die Kriterien dieses Tests bilden die in einem bestimmten Prüfstandard festgelegten Anforderungen.
Wichtige interne und externe Standards sind:

- Individuelle Vorgaben des Auftraggebers. Hier muß normalerweise geprüft werden, ob interne Sicherheitsrichtlinien eingehalten werden (wie beispielsweise der Schutz von Betriebsgeheimnissen).
- IT-Sicherheitsstandards, so wie sie in den Normen ISO 27001 oder dem IT-Grundschutz festgeschrieben beziehungsweise vorgeschlagen sind. Die ISO-Norm 27001 beschreibt die Anforderungen an ein Informationssicherheits-Management-System. Das Handbuch zum IT-Grundschutz wurde vom deutschen Bundesamt für Sicherheit in der Informationstechnologie (BSI) zusammengestellt. Dieser Leitfaden, der keine bindende, sondern nur eine vorschlagende Funktion haben darf, hat das Ziel, die Sicherheit der IT-Strukturen anhand konkreter Maßnahmen zu erhöhen.
- Gesetzliche Vorgaben. Hier ist in erster Linie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTrag) zu nennen, das die Vorstände von Aktiengesellschaften und Gesellschaften mit beschränkter Haftung dazu verpflichtet, geeignete Maßnahmen zu treffen, um frühzeitig existenzgefährdende Entwicklungen zu erkennen. Dabei handelt es sich insbesondere um die Einführung von Überwachungssystemen, wozu auch das IT-Risikomanagement zählt. Ein anderes Gesetz ist EURO-SOX, eine EU-Richtlinie, die auf dem amerikanischen SOX-Gesetz aufbaut. Es verlangt die Einrichtung eines internen Kontrollsystems, das die Wirksamkeit von internen Kontrollen, Revisionen und des Risikomanagements überwacht.

In der Regel wird bei einem Compliance-Test das interne IT-Risikomanagement auf Funktionstüchtigkeit geprüft. Als Referenz dient dabei die jeweilige Norm oder das entsprechende Gesetz.
Bei allen Compliance-Prüfungen dokumentiert der Tester die Vorgehensweisen und die Arbeitsergebnisse. Zum Schluß vergleicht er die Vorgaben mit den tatsächlich im Unternehmen verwirklichten Maßnahmen und ermittelt daraus den Grad der Einhaltung der Vorgaben.
Möchte sich ein Unternehmen beispielsweise nach dem IT-Grundschutz zertifizieren lassen, muß ein zertifizierter BSI-Auditor kontrollieren, wie viele der Maßnahmen aus dem IT-Grundschutz umgesetzt wurden. Dazu vergleicht er die relevanten Maßnahmen aus den IT-Grundschutz-Katalogen mit der tatsächlichen Situation im Unternehmen. Am Ende der Prüfung wird das prozentuale Verhältnis der umgesetzten Maßnahmen zur Gesamtmenge der Maßnahmen gebildet. Beträgt das Ergebnis mindestens zweiundachtzig Prozent, gilt der Compliance-Test zum IT-Grundschutz als bestanden und es kann ein Zertifikat ausgestellt werden.

Schwachstellenprüfung (Vulnerability Assessment)

Sollen potentielle Schwachstellen in einem Netzwerk aufgespürt werden – bedingt beispielsweise durch unsichere Zugriffskonfigurationen, den Betrieb unsicherer Software und den Verzicht auf Verschlüsselung –, ist ein Vulnerability Assessment durchzuführen. Bei diesem Testtyp übernehmen automatische Schwachstellenscanner den Hauptteil der Arbeit. Der Tester selbst wendet keine Energie auf, um das Netzwerk eigenständig zu erforschen oder Zugangsdaten zu erlangen. Damit dennoch ein verwertbares Ergebnis erbracht werden kann, müssen die Werkzeuge mit bestimmten Daten gefüttert werden. Diese Daten müssen von der Geschäftsleitung beziehungsweise einer berechtigten Person erfragt werden:

- Komplette Zugangsdaten oder mindestens die Zugangsdaten eines Basisanwenders passend zur Tiefe des Tests, damit die Werkzeuge prüfen können, welche Möglichkeiten ein Angreifer aufgrund von Benutzerrechten hat.
- Zugriff auf Netzwerkdiagramme und -schemata, damit die Werkzeuge das gesamte Ziel erfassen können.
- Voller Zugriff auf Konfigurationsdateien und Skripte, damit die Werkzeuge auch die Konfigurationsdateien überprüfen können.

Bei einer Schwachstellenprüfung wird zuerst mit den üblichen Mitteln auf dem üblichen Weg im System ein neuer IT-Benutzer angelegt (beispielsweise mit den Bordmitteln des Betriebssystems und der nachfolgenden Eintragung in einen Samba-, LDAP- oder Active-Directory-Verzeichnisdienst). Dieser muß über die Benutzerrechte verfügen, die dem Prüfziel entsprechen. Dann wird der Test mit den Zugangsdaten dieses Benutzers ausgeführt. Hier wird mit einem Schwachstellenscanner (wie Nessus, OpenVAS oder Nexpose) gearbeitet, dem die Ziele und Zugangskennungen übergeben werden. Das Werkzeug prüft dann die Authentifizierung des Users und seine De-facto-Berechtigungen. Als Ergebnis der Prüfungen wird ausgegeben, wo es Sicherheitslücken vorgefunden wurden.

Nicht ungewöhnlich ist es, daß es dabei zu irritierenden Warnungen und Falschmeldungen kommt. Der Grund ist meist in der Version eines Dienstes zu suchen. Insbesondere die Prüfergebnisse von Webanwendungen müssen auf Plausibilität geprüft werden, da die meisten Scanner aus dem Tritt kommen und eine Schwachstelle des Webservers vermuten, wenn die Anwendung keine Standard-HTTP-Antworten wie die bekannte Fehlermeldung »404 Website not found« generiert, sondern beispielsweise eine eigene Fehlermeldungsseite ausgibt. Solche Falschmeldungen muß der Tester in der Schlußdokumentation manuell eliminieren.

Als Ergebnis wird dem Auftraggeber die Auflistung der Risiken und des resultierenden Schadenpotentials in Berichtsform übergeben. Um seine Erkenntnisse und Schlußfolgerungen zu untermauern, sollte der Tester als Anhang die Ausgabe des Schwachstellenscanners mitliefern, wobei die offensichtlichen Falschmeldungen vorher entfernt oder zumindest markiert werden müssen.

Penetrations-Test

Ein Penetrations-Test ist eine Prüfung der aktuellen Sicherheit eines Programms (beispielsweise die Prüfung einer neuen Version der Online-Banking-Software auf mögliche Angriffsflächen) oder Netzwerks (beispielsweise die Überprüfung eines neu installierten drahtlosen Netzwerks mit Anschluß an das LAN, um sicherzustellen, daß kein unberechtigter Zugriff möglich ist).

In einem Penetrations-Test wird eine Schwachstellenprüfung um manuelle Prüfungen und Angriffe erweitert. Bei dieser Testform wird der Ausführende zum tragenden Element und nicht sein Werkzeug, er simuliert den Angriff eines Einbrechers oder böswilligen Anwenders.

Das erste Ziel eines Penetrations-Tests ist die Suche von Schwachstellen in Programmen und Netzwerkverbindungen. Werden welche gefunden, wird versucht, sie mit bestimmten Programmen auszunutzen und auf diesem Weg in das System einzudringen. Gelingt dies, dienen die gekaperten Systeme als Grundlage dafür, weiter in das Netzwerk vorzudringen und Zugangsdaten mitzuschneiden und vertrauliche Daten zu lesen.

Whitebox-Test

Eine Variante des Penetrations-Tests ist der Whitebox-Test. Hier erhält der Tester einen kompletten Zugriff auf die zu testenden Systeme, indem ihm vorab Detailinformationen zum Netzwerk und den zu testenden Systemen übergeben werden. Ein solcher Test ist recht schnell abgeschlossen, weil grob gesagt die Phase der Informationsgewinnung entfällt. Ein Whitebox-Text kann noch weiter dahingehend differenziert werden, ob das Ziel über den Angriff in Kenntnis gesetzt wird (Tandem Test) oder nicht (Reversal Test). Bei letzterem wird auch die Reaktion der Mitarbeiter beziehungsweise der Systeme auf den Angriff geprüft.

Blackbox-Test

Das Gegenstück zum Whitebox- ist der Blackbox-Test. Bei einem solchen erhält der Tester keine ausführlichen Informationen über das Testziel. Ihm wird lediglich der Name des Unternehmens, der Name einer Domain oder eine beliebige IP-Adresse genannt. Er muß dann versuchen, alle relevanten Daten über das zu testende Objekt selbst zu ermitteln, um dabei Schwachstellen zu finden. Auch bei diesem Testtyp kann unterschieden werden, ob das Ziel über den Angriff informiert ist (Blind Test) oder nichts vom bevorstehenden Test weiß (Double Blind Test).

Der Ablauf eines Blackbox-Tests entspricht dem eines Whitebox-Tests. Weil der Tester sein Ziel noch nicht kennt, muß er zuerst öffentlich verfügbare Informationen zur Zielfirma einholen. Bevorzugter Anlaufpunkt dafür ist die Homepage des Auftraggebers. Aus ihr kann er unter Umständen wichtige Informationen für einen Einbruch gewinnen.

Graybox-Test

Zwischen den White- und Blockbox-Tests ist der Graybox-Test angesiedelt. Als Ausgangspunkt für den Test der Systemsicherheit erhält der Tester denselben Zugriff auf das interne

Netzwerk wie ein Mitarbeiter ohne alle Details des Netzwerks zu kennen. Er muß alle relevanten Daten über das zu testende Objekt selbst herausfinden. Hier besteht ebenfalls wieder die Option das Ziel über den Test, den Zielbereich und den Zeitrahmen zu informieren (Graybox Test) oder nicht (Double Graybox Test).
Der Ablauf eines Graybox-Tests entspricht dem eines Blackbox-Tests, jedoch mit dem Unterschied, daß der Tester soweit über das Ziel in Kenntnis gesetzt wurde wie auch ein interner Mitarbeiter mit normalen Benutzerrechten das Ziel kennt und über entsprechende Zugangsberechtigungen verfügt.
In seinem Abschlußbericht dokumentiert der Penetrations-Tester seine Vorgehensweisen und die Ergebnisse. Um seine Ergebnisse zu untermauern, muß er dem Auftraggeber eine Übersicht über die Tests zusammenstellen, in der die Zielsysteme, der Zeitrahmen sowie die Werkzeuge und Techniken genau aufgeführt werden. Neben den Testergebnissen muß er auch die daraus resultierenden Gefährdungen präsentieren.

1.1.2 Methodik

Werden in Computersystemen Sicherheitslücken gefunden, läßt sich anhand ihrer Menge und ihrer Auswirkung eine theoretische Aussage über das Sicherheitsniveau der getesteten Systeme zum Zeitpunkt der Prüfung treffen. Allerdings hängt das Auffinden von vorhandenen Sicherheitslücken stark vom Vorgehen und Können des Testers ab. Ein Tester, der kein Know-how zu Unix-Systemen hat, wird sich schwertun, solche Systeme erfolgreich zu prüfen. Seine Ergebnisse werden sicherlich von denen eines erfahrenen Unix-Testers abweichen. Es kann sogar passieren, daß eine bekannten Schwachstelle schlichtweg übersehen wird und er deswegen zu einem falschen Ergebnis kommt.
Erschwerend kommt hinzu, daß Testergebnisse nicht unwesentlich von der Vorgehensweise abhängen, in der die Systeme geprüft werden. Ein- und derselbe erfahrene Tester wird bei der mehrfachen Prüfung desselben Systems bei einer anderen Vorgehensweise zu unterschiedlichen Ergebnissen kommen.
Um solche inakzeptablen Unwägbarkeiten bei einem Penetrations-Test auszuschalten, müssen sich die Testreihen gemäß einer generelle Vorgehensweise durchgeführt werden, die garantiert, daß:

- Der Test gründlich durchgeführt wird.
- Der Test alle erforderlichen (Kommunikations-)Kanäle umfaßt.
- Der Test gesetzeskonform ist.
- Die Ergebnisse meßbar sind.
- Die Ergebnisse konsistent und wiederholbar sind.
- Der Test nur Schlußfolgerungen enthält, die aus dem Test selbst abgeleitet sind.

Das einzige Handbuch, das all diese Anforderungen abdeckt und das sich bei der Arbeit des Autors bewährt hat, ist das Open Source Security Testing Methodology Manual (OSSTMM). Sein Hauptziel ist die Erarbeitung einer wissenschaftlichen Methode zur genauen Bestimmung der tatsächlichen Sicherheit (in OSSTMM »operative Sicherheit«, kurz

OPSEC, genannt) mittels Untersuchung und Korrelation der Testergebnisse in einer konsistenten und zuverlässigen Weise. Das Handbuch wurde von der Isecom (http://www.isecom.org/osstmm/) entwickelt, diese bezeichnet sich selbst als offene, kooperative, Non-Profit-, Wissenschafts- und Sicherheits-Forschungsorganisation. Registriert ist sie in Spanien. Ihre Forschungsbemühungen sind nach eigenen Angaben ohne kommerziellen oder politischen Einfluß, ihr Ziel ist es, praktische Methoden und Messungen für Sicherheit und Integrität anzubieten, die vom Vorstandsmitglied bis zum Schüler verstanden werden. Zu diesem Zweck arbeitet Isecom mit Schulen, Universitäten, Unternehmen und Regierungsbehörden zusammen.

Das Handbuch bietet eine Methodik zur Durchführung von Sicherheitsanalysen (OSSTMM-Audits), um den Grad der die Sicherheit auf operativer Ebene genau messen zu können. Dabei werden subjektive Vermutungen oder Annahmen ausgeschaltet. Es gibt eine methodische Vorgehensweise vor, denn nur ein fester Testablauf kann automatisch wiederholbare und konsistente Ergebnisse liefern.

In Anhang A dieses Buchs ist der Ablauf eines OSSTMM-Audits an einem Beispiel vorgestellt, die einzelnen OSSTMM-Testphasen werden jeweils an einem externen und internen System gezeigt.

Im OSSTMM-Audit werden zuerst die ansprechbaren Systeme gesucht. Werden welche gefunden – in der Sprache des OSSTMM heißt ein gefundenes System Visibility –, werden sie in ein Formblatt eingetragen. Ebenso werden die im Test gefundenen Sicherheitslücken– als solche gelten nicht nur technische Verwundbarkeiten, sondern Informationspreisgaben durch Mitarbeiter –, in dem Blatt vermerkt. Zudem sind die bereits installierten Sicherheitsmaßnahmen in das Formelblatt aufzunehmen. Als Ergebnis liefert das Formular den Risk Assessment Value (RAV) des Testobjekts. Das ist eine Prozentzahl, die das vorgefundene Sicherheitsniveau in Relation zum nur in der Theorie erreichbaren Maximalwert von 100 Prozent ausdrückt. Die Höhe des Meßwerts ist die Grundlage für die Bewertung eines Systems als *sicher* beziehungsweise *unsicher*. Alle Schwächen bedeuten Abschläge von diesem Wert. Erst ein System ab einem RAV von 90 Prozent kann per definitionem als sicher eingestuft werden.

Der berechnete Meßwert läßt sich auch grafisch darstellen, Bild 1.1 zeigt ein Beispiel. In einer grafischen Aufbereitung kann das Sicherheitsniveau – vielleicht sogar im Lauf der Zeit – eingängig abgebildet werden. Um den Wert zu verdeutlichen, schadet es auch nicht, ihn in Relation zu beispielsweise früheren Testergebnissen oder Industriestandards zu setzen.

Weil die Gefährdungen (wie Sicherheitslücken und Informationsabflüsse) und die Sicherheitsmechanismen (wie Authentifizierung und Verschlüsselung) im Modell erfaßt werden, kann nicht nur die Sicherheit des Systems bewertet, sondern es kann auch mit anderen Systemen verglichen werden. Unterzieht man die Details der festgestellten Gefährdungen und Sicherheitsmechanismen einer genauen Analyse, kann festgestellt werden, wo Kontrollfunktionen nicht wie vorgesehen funktionieren oder wo Schwachstellen vorhanden sind.

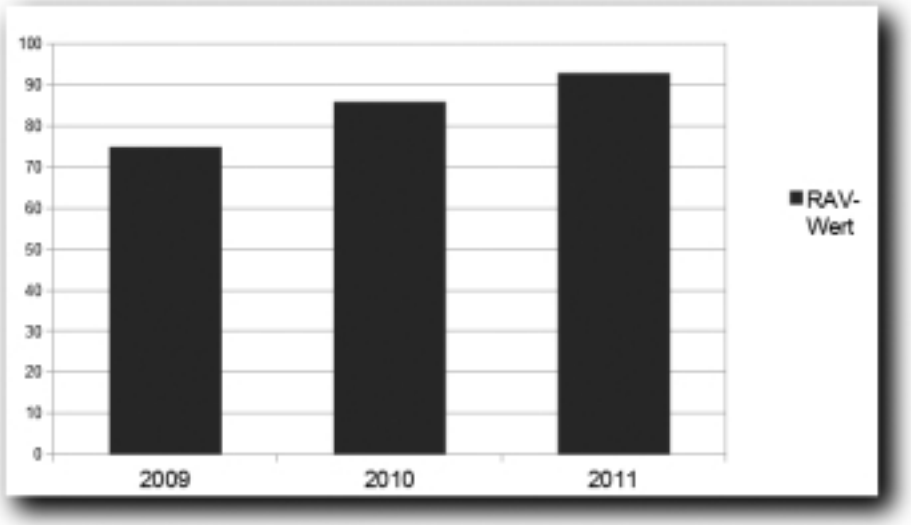


Bild 1.1: Die grafische Darstellung eines Risk Assessment Value (RAV)

Um eine möglichst hohe operative Sicherheit eines Systems zu erreichen, müssen die potentiellen Gefährdungen entweder vom operativen System getrennt werden – beispielsweise durch Trennung der Netzverbindung – oder kontrolliert werden, beispielsweise durch einen Zugangsschutz.

Sicherheitsfaktoren

Eine Sicherheit von vollen einhundert Prozent können nur solche Systeme erreichen, die vollständig von einem Netzwerk getrennt sind. Das können also ausschließlich Standalone-Computer sein, und die noch ohne Laufwerke, so daß über keinen Datenträger Schadcode in das System eindringen kann. Das wird in einem Unternehmen nie der Fall sein, jeder Arbeitsplatz-PC wird in irgend einer Form mit seiner Umwelt kommunizieren müssen.
Überall dort, wo ein System nicht komplett von einem Netzwerk getrennt ist, bestehen Interaktionsmöglichkeiten mit anderen Systemen. Jede mögliche Interaktion reduziert die Systemsicherheit automatisch unter hundert Prozent. Die Interaktionsmöglichkeiten werden im OSSTMM-Audit in drei Bereichen untersucht:

- Die Sichtbarkeit (Visibility). Als Visibility zählen die Systeme, die auf einen Ping oder einen ansprechbaren Dienst antworten. Diese müssen gezählt werden, die Anzahl muß notiert werden.
- Das Vorhandensein von Kommunikationspunkten (Access). Dies sind die ansprechbaren Dienste auf einem System. Auch ihre Anzahl wird notiert.
- Die Vertrauensbeziehungen zwischen Systemen (Trust). Darf beispielsweise der Webserver mit einem E-Shop automatisiert auf den Datenbankserver zugreifen, zählt dies als ein Trust. Die Anzahl der Trusts wird notiert.

Zum Schluß werden die einzelnen Posten zusammengezählt. Das Ergebnis ist die Summe der Interaktionsmöglichkeiten. Sie bezeichnet die Durchlässigkeit eines Systems (Porosity).

Kontrolle

Um die Auswirkung von Bedrohungen durch Interaktionsmöglichkeiten in Schach zu halten, sind in jedem Unternehmen bestimmte Kontrollmechanismen installiert, die in interaktive und defensive Mechanismen unterschieden werden.

Interaktive Kontrollmechanismen haben direkten Einfluß auf die drei Eckpfeiler der operativen Sicherheit Visibility, Access und Trust und werden der **Klasse A** zugeordnet.

In diese Klasse gehören:

- Die **Authentifizierung:** Ein Benutzer wird anhand von Zugangsdaten identifiziert oder autorisiert.
- Die **Absicherung:** Das ist eine zusätzliche Schutzmaßnahme als Vereinbarung in Form einer Warnmeldung oder Lizenz zwischen dem Systembesitzer und dem interaktiven Teilnehmer oder eine Versicherung gegen Computerschäden.
- Die **Vorgaben:** Sie bestimmen verbindlich, wie interagiert werden soll, wobei der Kommunikationspartner keine Möglichkeit hat, die Art der Interaktion zu wählen, weil sie erzwungen wird, beispielsweise eine verschlüsselte Verbindung.
- Die **Kontinuität:** Auch im Falle eines Ausfalls oder Fehlers bleiben alle Dienste verfügbar.
- Die **Widerstandsfähigkeit:** Im Falle eines Ausfalls oder Fehlers funktionieren die anderen Sicherheitsvorkehrungen weiterhin und fallen nicht aus; beispielsweise wenn eine Blockall-Funktionalität in einer Firewall nicht davon betroffen ist, wenn es auf der Firewall zu Fehlern kommt.

Defensive Kontrollmechanismen werden in der **Klasse B** abgebildet. Sie beeinflussen nicht direkt die Interaktionen, sondern stellen Schutzmaßnahmen im Fall einer Gefährdung dar.

Zu ihnen zählen:

- Die **Unabstreitbarkeit:** Die Teilnehmer einer Interaktion werden eindeutig identifiziert und protokolliert, beispielsweise durch Logging oder Monitoring. Das Ziel ist, daß niemand die Teilnahme an der Interaktion leugnen kann.
- Die **Vertraulichkeit:** Sie garantiert die Vertraulichkeit der übermittelten Daten einer Interaktion, beispielsweise eine Verschlüsselung über SSH oder SSL.
- Die **Geheimhaltung:** Nur die beteiligten Personen wissen, wo der Informationsaustausch stattfindet; Beispiele sind Port-Knocking oder das Betreiben von Diensten abseits der Standardports.
- Die **Integrität:** Die Kommunikationspartner werden informiert, falls sich Daten während des Austauschs geändert haben; üblicherweise wird die Integrität durch Verschlüsselung oder Prüfsummen sichergestellt.
- Der **Alarm:** Er meldet eine (anhaltende) Interaktion.

Sicherheitslücken

Werden in einem System Sicherheitslücken gefunden, haben diese unterschiedliche Auswirkungen. Ihre möglichen Folgen auf die Sicherheit müssen im Rahmen des OSSTMM-Audits bewertet werden. Darin werden fünf Varianten von Sicherheitslücken unterschieden:

- **Kritische Lücken (Vulnerability)** können folgende Auswirkungen haben:
  (a) Sie blockieren auch autorisierten Personen oder Prozessen den Zugang zu einem System,
  (b) sie erlauben auch unautorisierten Personen oder Prozessen privilegierten Zugriff und/oder
  (c) unautorisierte Personen oder Prozesse können die eigenen Aktivitäten verschleiern.
- **Schwachstellen (Weakness)** vermindern die Wirksamkeit eines Kontrollmechanismus der Klasse A oder heben ihn sogar auf.
- **Bedenken (Concern)** vermindern die Wirksamkeit eines Kontrollmechanismus der Klasse B oder heben ihn sogar auf.
- **Informationspreisgabe (Exposure)** macht Ziele direkt oder indirekt sichtbar. Dazu zählt beispielsweise die Anzeige von Versionsnummern von Diensten.
- **Anomalie (Anomaly)** ist ein unidentifiziertes oder unbekanntes Problem, das nicht kontrolliert und im normalen Betrieb berücksichtigt werden kann.

Category		OPSEC	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

Bild 1.2: Die Einordnung einer Schwachstellen in eine Kategorie (Quelle: OSSTMM)

Die Sicherheitslücken werden fünf Kategorien zugeordnet:

- Ist die Sichtbarkeit (Visibility) betroffen, handelt es sich um eine Schwachstelle aus dem Bereich Informationspreisgabe (Exposure).
- Wirkt sich die Schwachstelle auf Kommunikationspunkte (Access) oder Vertrauensbeziehungen (Trust) aus, handelt es sich um eine kritische Lücke (Vulnerability).

- Sind die Kontrollmechanismen der Klasse A betroffen, wird von einer Schwachstelle (Weakness) gesprochen.
- Sind die Kontrollmechanismen der Klasse B beeinflußt, handelt es sich um ein Bedenken (Concern).
- Unklarheiten werden als Anomalie vermerkt.

Bild 1.2 stellt dar, nach welchen Gesichtspunkten eine im Test gefundene Schwachstelle einer der fünf genannten Kategorien zugeordnet wird. So würde beispielsweise ein Telnet-Zugang ohne Paßwortabfrage eine Schwachstelle im Bereich Kommunikation (Access) darstellen und ist als kritische Lücke (Vulnerability) zu werten.

1.1.3 Audit

Ein OSSTMM-Audit besteht aus mehreren Komponenten: der Planungsphase, der Ablaufphase und der Berechnung des Risikofaktors.

Planungsphase

In der Planungsphase ist zunächst zu definieren, welche Systeme einer Sicherheitsbestimmung zu unterziehen sind. Diese Systeme werden in einem OSSTMM-Audit *Assets* genannt. Die eigentlichen Ziele des Tests sind die Schutzmaßnahmen dieser Assets, denn letztlich entscheiden diese darüber, ob ein System sicher ist oder nicht.

Außer den Assets selbst müssen ihre Umgebung, ihre Schutzmechanismen und die umgebenden Prozesse betrachtet werden, weil diese mit den Assets interagieren. Sie bilden den Bereich, in dem die Zielsysteme miteinander kommunizieren.

Ebenso muß alles untersucht werden, was benötigt wird, um die Zielsysteme am Laufen zu halten. Dazu zählen neben der Infrastruktur auch Prozesse, Protokolle und Ressourcen. Sie bilden den Zielbereich (Scope) des Tests. In diesem arbeitet später der Tester.

Auch die Interaktionen innerhalb des Zielbereichs und zwischen dem Zielbereich mit der Außenwelt müssen analysiert werden. Diese Interaktionswege werden logisch in Richtungen unterteilt, beispielsweise von innen nach außen, von außen nach innen, Abteilung A zu Abteilung B und so weiter. Diese einzelnen Interaktionswege heißen Vektoren. Jeder Vektor muß eigens untersucht werden.

Dann müssen die Interaktionsmöglichkeiten jedes Vektors herausgefunden werden. Diese werden in fünf Kanäle und drei Klassen unterschieden:

In der Klasse der physikalischen Sicherheit sind die Kanäle Mensch und Gerät angesiedelt; in dieser Klasse geht es um die Täuschung von Anwendern und den Einbruch und Diebstahl von Systemen. Die Klasse der Spektrumsicherheit betrifft die drahtlosen Übertragung, es wird jede elektrische Kommunikation, Signalübertragung oder Ausstrahlungen in den elektromagnetischen Bereichen analysiert. Die Kommunikationssicherheit ist die dritte Klasse ab und umfaßt die Telekommunikation und Datenkommunikation, sprich: die Telefonie und Datenübertragung. Jeder in einem Vektor identifizierte Kanal muß einzeln getestet werden.

Abschließend muß das genaue Ziel des Tests festgelegt werden: Sollen nur die Interaktionsmöglichkeiten getestet werden oder auch die Reaktion der vorhandenen Sicherheitsmaßnahmen? Die Antwort auf diese Frage bestimmt den Testtyp. Dieser ist für jeden aus dem obigen Schema abgeleiteten Test individuell zu bestimmen.
Zu guter Letzt muß sichergestellt werden, daß der geplante Test mit den im OSSTM definierten Regeln (Rules of Engagement) konform ist. Diese geben ethische und organisatorische Hinweise zum OSSTMM-Audit. Die Regeln sind sehr umfangreich, hier kann nur eine grobe Übersicht gegeben werden. So soll bei der Auftragsbeschaffung seriös um Kunden geworben werden. Angst machen oder öffentliche Hackervorführungen sind untersagt. Aufträge dürfen nur mit schriftlicher Genehmigung des Ziels angenommen werden. Zudem dürfen offensichtlich unsichere Systeme gar nicht erst getestet werden. Bei der Vertragsgestaltung sind der Zielbereich und die Grenzen schriftlich zu fixieren, dem Auftraggeber muß ein Testplan vorgelegt werden. Auch zum Testvorgang selbst finden sich diverse Vorschriften wie die Einhaltung der Gesetze. Zum Schluß wird der Abschlußbericht unter die Lupe genommen, unter anderem wird vorgeschlagen, was er enthalten muß und wann die Privatsphäre von Personen zu berücksichtigen ist.

Ablauf

Ein OSSTMM-Audit besteht aus mehreren Phasen.

Phase 1: Einleitungsphase
Die Einleitungsphase des Audits beginnt mit dem Definieren der Anforderungen, des Zielbereichs und der Testeinschränkungen. Zu berücksichtigen sind dabei die Firmenkultur und Vorgaben aus Normen, Gesetzen und Richtlinien. Damit die Messungen technisch nachvollziehbar sind, muß geprüft werden, welche Auswirkungen die Qualität der Netzverbindung und der räumliche Abstand zum Ziel auf die Testergebnisse hat beziehungsweise haben könnte. Als letztes wird getestet, ob technische Maßnahmen vorhanden sind, die auf den Versuch Interaktionen zu finden reagieren. Mit anderen Worten: Es werden die Einbruchserkennungs-Systeme identifiziert.

Phase 2: Interaktionsphase
In der Interaktionsphase werden die sichtbaren Ziele im Zielbereich ermittelt (Visibility Audit). Dann wird geprüft, welche Kommunikation mit den Zielen möglich ist (Access Verification). Zudem werden die Vertrauensbeziehungen zwischen den einzelnen Zielen ermittelt (Trust Verification) und die Kontrollmechanismen der Klasse B getestet (Control Verification).

Phase 3: Prüfungsphase
Die Ergebnisse der Prüfungsphase hängen stark von den Informationen ab, die der Tester vorab sammeln konnte beziehungsweise die ihm übergeben wurden. Zuerst wird geprüft,

STICHWORTVERZEICHNIS

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z