Enno Rey
Michael Thumann
Dominick Baier

Mehr IT-Sicherheit durch Pen-Tests

- Optimierung der IT-Sicherheit durch gelenktes „Hacking“
- Von der Planung über die Vertragsgestaltung zur Realisierung

Mit Online-Service zum Buch

vieweg

Edition <kes>

Enno Rey
Michael Thumann
Dominick Baier

Mehr IT-Sicherheit durch Pen-Tests

Edition <kes>

Herausgegeben von Peter Hohl

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes> – Die Zeitschrift für Informations-Sicherheit (s. a. www.kes.info), die seit 1985 im SecuMedia Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

Die ersten Titel der Reihe:

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheit – Make or Buy
Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

www.vieweg-it.de

Enno Rey
Michael Thumann
Dominick Baier

Mehr IT-Sicherheit durch Pen-Tests

Optimierung der IT-Sicherheit durch gelenktes „Hacking“ – Von der Planung über die Vertragsgestaltung zur Realisierung

Herausgegeben von Stephen Fedtke

vieweg

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage März 2005

Alle Rechte vorbehalten
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011, Softcover 2013

Lektorat: Dr. Reinald Klockenbusch / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.
www.vieweg-it.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de
Umschlagbild: Nina Faber de.sign, Wiesbaden
Druck und buchbinderische Verarbeitung: Wilhelm Adam, Heusenstamm
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

ISBN 978-3-528-05839-5 (Hardcover)
ISBN 978-3-8348-2626-8 (Softcover)
e-ISBN 978-3-322-80257-6
DOI 10.1007/978-3-322-80257-6

Vorwort

Neben der Definition der eigenen Sicherheits-Bedürfnisse und der Umsetzung von Schutz-Massnahmen (seien sie technischer, organisatorischer oder vertraglicher Natur) gehört zu einem funktionierenden Sicherheits-Regelkreis immer auch das regelmässige Hinterfragen, ob etwa die definierten Ziele mit den getroffenen Massnahmen auch erreicht werden. Zu den dafür notwendigen Kontroll-Mechanismen zählen Penetrations-Tests, die damit einen wichtigen Platz innerhalb der IT-Sicherheit haben.

Inhalt dieses Buchs sind in erster Linie die Tools und Techniken von Angreifern, mithin das Handwerkszeug eines Pentesters. Zu formalen Rahmenbedingungen oder methodischen Fragen liegen mit der BSI-Studie *Durchführungskonzept für Penetrationstests* oder dem von Pete Herzog initiierten *Open Source Security Testing Methodology Manual* (OSSTMM) umfassendere Werke vor. Wir möchten uns auf Angriffs-Methoden konzentrieren und folgen hier einer strikten *Full Disclosure* Politik, d. h. wir halten eine öffentliche Darstellung oder detaillierte Diskussion von Angriffen für sinnvoll zur Ausbildung hohen Sicherheits-Knowhows, sei es auf Seiten von Prüfern, sei es auf Seiten von Sysadmins (die daher explizit auch zum intendierten Adressatenkreis des Buchs zählen). Es sollte sich von selbst verstehen, dass alle beschriebenen Methoden nur gegen Systeme eingesetzt werden sollten, bei denen Sie dazu qua erteiltem Auftrag oder beruflicher Funktion autorisiert sind.

Wir wünschen allen Lesern viel Freude und spannende Momente bei der Lektüre. Für Anregungen fachlicher Art, Hinweise auf Fehler oder auch nur eine einfache Rückmeldung, welche Kapitel Ihnen besonders gefallen haben, sind wir stets dankbar und nehmen all dies gerne unter der Mail-Adresse pentest-buch@ernw.de entgegen.

Heidelberg im Februar 2005,

Dominick Baier

Enno Rey

Michael Thumann

Inhaltsverzeichnis

1 Sinn und Zweck von Penetrations-Tests

Improving the Security of Your Site by Breaking Into it – so lautete der Titel eines 1993 von Dan Farmer und Wietse Venema im Usenet geposteten Papers [1], in dessen Folge sie dann auch den ersten frei verfügbaren Vulnerability-Scanner (*SATAN, Security Administrator Tool for Analyzing Networks*) veröffentlichten.

Genau das ist auch Anliegen eines Penetrations-Tests: eine Verbesserung der IT-Sicherheit[1] als Folge des aktiven Versuchs, in Netze oder Systeme einzudringen.

Dies ist zumindest der Ideal-Fall: Nicht immer werden Penetrations-Tests beauftragt, um auch tatsächlich die Sicherheit der geprüften Systeme zu verbessern. Zuweilen will der Auftraggeber auch nur internen Vorgaben oder von höherer Stelle geäusserten Wünschen entsprechen, ohne an einer konkreten Umsetzung von Empfehlungen interessiert zu sein. Wir sind immer wieder überrascht, vielfach bei turnusmässig wiederholten Prüfungen exakt dieselben Lücken zu finden, die wir etwa bereits im Vorjahr moniert hatten oder im Jahr davor oder ...

Unsere Arbeits-Definition des Terminus *Penetrations-Test* sieht diesen als den „zielgerichteten Versuch, mit den Mitteln eines Angreifers und innerhalb einer gegebenen Zeitspanne Lücken in der IT-Sicherheit aufzudecken."

Ziel ist also, gewissermassen durch Simulation eine bestimmte Klasse von Risiken zu prüfen, nämlich die Klasse der logischen Angriffe gegen Systeme oder Netze. Diese Prüfung findet nicht durch lesende Untersuchung der System-Konfiguration oder durch Interviews statt – beides typische Methoden klassischer Audits – sondern eben mit den „Mitteln eines Angreifers", das

[1] Dem Leser bleibt überlassen, hier gedanklich verwandte Begriffe wie etwa *Information Security* zu verwenden. Eine Diskussion der (überdies regelmäßig wechselnden) Spielarten des *Sicherheits-* oder *Security*-Begriffs soll hier nicht stattfinden.

E. Rey et al., *Mehr IT-Sicherheit durch Pen-Tests*,
DOI 10.1007/978-3-322-80257-6_1,
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

sind üblicherweise Tools und Techniken. Der genannte „Angreifer" kann dabei ganz unterschiedlicher Natur sein (Mitbewerber, frustrierter (Ex-) Mitarbeiter, Krimineller etc.) und die ggf. unterschiedliche Definition dieses „Angreifers" hat oft auch Auswirkung auf das Vorgehen während des Tests und die Art der Ergebnisse. Die (zwischen Auftraggeber und Prüfer) gemeinsame Definition des „Angreifers" gehört daher auch zu den ersten und wichtigsten Schritten eines Tests. Privatbanken im europäischen Ausland mit divergierender Steuer-Gesetzgebung etwa haben eine völlig andere Sicht eines möglichen „Angreifers" als beispielsweise Hersteller von Nahrungsmitteln mit genmanipulierten Anteilen („deutsche Steuerfahndung oder investigativer Journalist" im ersten Fall, „politisch motivierter Aktivist" im zweiten).

Die Prüfung[2] ist (aufgrund des Auftrags-Charakters) zeitbegrenzt, was den einzigen Unterschied zum Vorgehen eines tatsächlichen „Angreifers" konstituieren sollte. Der Pentester kann dieser Einschränkung naturgemäß nicht entrinnen (es sei denn, er würde sich jenseits des Auftrags oder seiner Prüf-Ethik [siehe dazu unten] verhalten). Es ist aber hilfreich, sich diese Einschränkung regelmässig wieder ins Gedächtnis zu rufen bzw. sie an geeigneter Stelle auch im Bericht zu erwähnen. Ein im Rahmen des Tests „negatives" Ergebnis (etwa ein *nicht* geknacktes Kennwort) muss für den tatsächlichen Angreifer ohne zeitliche Beschränkung durchaus kein Hindernis darstellen.

Ergebnis des Tests sollte die Identifizierung von Schwachstellen sein (oder auch die Feststellung, dass keine solchen aus Sicht des „Angreifers" erkennbar sind), die dann ggf. nach einer Risiko-Bewertung behoben werden sollten, womit eben die Gesamt-Sicherheit potentiell verbessert wird.

Neben der Definition der eigenen Sicherheits-Bedürfnisse und der Umsetzung von Schutz-Massnahmen (seien sie technischer, organisatorischer oder vertraglicher Natur) gehört zu einem funktionierenden Sicherheits-Regelkreis immer auch das regel-

---

2 Wir verwenden im folgenden die Begriffe *Penetrations-Test*, *Pentest*, *Test* oder *Prüfung* völlig austauschbar.

mässige Hinterfragen, ob etwa die definierten Ziele mit den getroffenen Massnahmen auch erreicht werden. Zu den dafür notwendigen Kontroll-Mechanismen zählen Penetrations-Tests, die damit einen wichtigen Platz innerhalb der IT-Sicherheit haben.

2 Standards und rechtliche Aspekte

Im Gegensatz zur IT-Revision, innerhalb derer bei der Durchführung von Audits durch gesetzliche Vorgaben (schon zur Revision selbst) und durch die Prüfziele[3] Gegenstand und Form eines Audits weitgehend determiniert sind, ist der formale Rahmen von Penetrations-Tests nur wenig eingeschränkt.

Es gibt keine verbindlichen Standards zu Ablauf, Methodik oder Dokumentation von Pentests, und auch der rechtliche Rahmen kann – insbesondere bei Tests im internationalen Umfeld – nicht durchweg eindeutig bewertet werden. Gleichwohl befindet sich der Prüfer nicht völlig im ‚luftleeren Raum', und wir wollen hier kurz Hinweise zur formalen Ausgestaltung von Tests und zu Rahmenbedingungen für das Verhalten des Testers geben.

2.1 Standards

Seit einigen Jahren gibt es verschiedene Versuche, eine standardisierte Vorgehensweise für Penetrations-Tests zu beschreiben:

- das *Open Source Security Testing Methodology Manual, OSSTMM* (s.o.)
- die BSI-Studie *Durchführungskonzept für Penetrationstests* (s.o.)
- die *Guideline on Network Security Testing* des US-amerikanischen *National Institute of Standards and Technology* (NIST) [1]

Prüfer, die auf eine von Praktikern erarbeitete *Best Practice*-Methodik zurückgreifen oder die die eigene, bereits praktizierte Vorgehensweise überdenken oder erweitern wollen, sollten sich am ehesten am *OSSTMM* orientieren, ggf. kann hier die BSI-Studie zusätzlich hilfreich sein. Beide bieten auch (im Ggs. zum

[3] Etwa die Prüfung der Ordnungsmäßigkeit und Sicherheit des DV-gestützten Buchführungsprozesses.

E. Rey et al., *Mehr IT-Sicherheit durch Pen-Tests*,
DOI 10.1007/978-3-322-80257-6_2,
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

NIST-Dokument) Checklisten, die zur Unterstützung der eigenen Arbeit herangezogen werden können.

Die von Seiten des Auftraggebers oft gestellte Frage, nach welchem Standard man denn arbeite, lässt sich mit Verweis auf das *OSSTMM* nach unserer Erfahrung nur unzureichend beantworten. Hier ist oft ein Verweis auf „die BSI-Methodik" oder eine Bemerkung der Art „we're working in compliance to the NIST Guideline" definitiv die bessere Antwort. Selbst wenn es sich beim NIST-Dokument streng genommen um ein *Draft* handelt und es zudem nur wenig konkrete, strukturierte Handlungs-Anweisungen gibt, hat allein die Erwähnung des NIST bei amerikanischen Unternehmen oft erhebliches Gewicht (vergleichbar etwa dem im deutschsprachigen Raum immer noch vorhandenen Glauben an die Autorität des BSI und des *Grundschutzhandbuchs*).

2.2 Rechtliche Aspekte

Die Durchführung von Penetrations-Tests birgt Risiken sowohl für den Auftraggeber (Offenlegung sensibler Daten gegenüber Dritten [dem Pentester][4], Produktivitäts-Verlust durch System-Ausfall) wie auch für den Prüfer (Haftungs-Fragen bei Verursachung von Produktivitäts-Verlusten oder strafrechtliche Bestimmungen bei der unautorisierten Prüfung von Systemen). Es sollten daher im Vorfeld des Tests bilaterale Regelungen getroffen werden, die diese Risiken und das enthaltene Konfliktpotential minimieren. Das kann innerhalb des den Auftrag konstituierenden Vertrags sein oder in Form eines dedizierten, separaten Dokuments stattfinden.

Eine diesbezügliche Vereinbarung sollte u.a. enthalten:

- eine Vertraulichkeitserklärung des Testers: Diese wird von vielen Auftraggebern oft sowieso schon in sehr frühem Stadium der Zusammenarbeit gefordert, und es gibt dafür meist auch dedizierte Dokumente seitens der Auftraggeber,

[4] Man könnte einwenden, dass eine solche Offenlegung ein immanentes Risiko des Kontrollwerkzeugs Penetrations-Test ist. Allerdings hat der Auftraggeber auch in seiner Organisation für die Einhaltung datenschutzrechtlicher Vorschriften oder des Betriebsverfassungsgesetzes zu sorgen, und hier kann es durchaus zu Kollisionen mit den Ergebnissen des Tests kommen (deren Behandlung dann eben geregelt sein muss).

- eine Verpflichtung zu sorgfältigem und verantwortungsbewusstem Handeln[5] (etwa in Form einer formulierten *Prüf-Ethik*, siehe dazu 2.3),
- ein Haftungs-Ausschluss für den Auftragnehmer,
- die Erklärung des Auftraggebers, für die getesteten Systeme zuständig zu sein oder über das Einverständnis der jeweiligen *System Owner* zu verfügen.

Wir können an dieser Stelle kein Muster einer solchen Regelung veröffentlichen, um die Grauzone der Rechtsberatung zu vermeiden. Der interessierte Leser sei aber an die BSI-Studie (die dem Thema eine umfangreiche Erörterung widmet) oder an einschlägige Fach-Anwälte verwiesen.

Besonders problematisch werden diese Aspekte, wenn Sie im internationalem Unfeld testen. Hier gilt als Faustregel, dass der Prüfer versuchen sollte, die Durchführung von Tests soweit wie möglich *im* Land des Standorts der Systeme durchzuführen (also *nicht* über Landesgrenzen hinweg) und um ergänzende Regelungen/Dokumente nachzusuchen, die von Vertretern im jeweiligen Land unterzeichnet sind und ggf. auf dortige Bestimmungen Bezug nehmen.

2.3 Prüf-Ethik

Über gesetzliche Vorgaben oder Rahmenbedingungen hinaus sollte der Prüfer sein Handeln an hohen ethischen Anforderungen ausrichten und regelmässig vor dem Hintergrund solcher hinterfragen. Auch bei Problem-Situationen innerhalb des Tests kann eine gemeinsame Diskussion vor dem Hintergrund solcher Verhaltensrichtlinien zuweilen sinnvoll und klärend sein. Typische Beispiele entsprechender Verhaltens-Kodizes sind die, die für Mitglieder einschlägiger Berufs-Organisationen (etwa der ISACA[6]) oder Inhaber der zugehörigen Zertifizierungen verbindlich sind. Für einen *CISSP* ist das etwa der *Code of Ethics* von

---

5 Ein solches Handeln sollte man seitens des Testers voraussetzen können. Hier spielt aber auch der psychologische Aspekt für den Auftraggeber (der ja eben die o.g. Risiken auch sieht, insbesondere für die Verfügbarkeit oder hinsichtlich des Konfliktpotentials mit dem BetrVG und seinen Vertretern) eine nicht zu unterschätzende Rolle.

6 *Information Systems Audit and Control Association*

ISC² [2], für einen *CISA* der *Code of Professional Ethics* der ISACA [3].

Ein gutes (deutschsprachiges) Beispiel sind die *Ethischen Grundsätze* der *Fachgruppe Security* der *Schweizerischen Informatikgesellschaft* [4], die wir deshalb auch hier zitieren:

Wir wollen:

- die im Verlaufe unserer Tätigkeit erhaltenen Informationen schützen und diese weder zum persönlichen Vorteil nutzen noch unberechtigten Parteien zugänglich machen;
- bei unseren Tätigkeiten gebührende Vorsicht walten lassen;
- nur solche Aufgaben übernehmen, für die wir durch Ausbildung oder Erfahrung genügend qualifiziert sind;
- laufend das Verständnis und die Fachkompetenz für Methoden und Technologien, ihre korrekte Anwendung und die möglichen Konsequenzen verbessern;
- Informationen mit genügender Professionalität sammeln und auf der Basis dieser Informationen ehrlich und realistisch sein bei der Deklaration von Feststellungen und Empfehlungen;
- unsere Aufgaben unabhängig und objektiv durchführen;
- echte und empfundene Interessenskonflikte wo immer möglich vermeiden und sie den Betroffenen mitteilen, wenn solche vorkommen;
- jegliche Handlungen vermeiden, welche Dritte in ihrem Besitz oder ihrem Ruf verletzen;
- Bestechungen in jeglicher Form ablehnen und nie wissentlich an illegalen oder inkorrekten Handlungen teilnehmen;
- ehrliche Kritik der Arbeiten suchen und akzeptieren; Fehler bestätigen und korrigieren und fair die Leistungen Dritter erwähnen;
- die Aufstellung und Einhaltung angemessener Standards, Verfahren und Kontrollen für unsere Tätigkeiten unterstützen;

- unsere Kollegen und Mitarbeiter in ihrer professionellen Entwicklung unterstützen und ihnen bei der Einhaltung dieser ethischen Grundlagen helfen.

3 Ablauf eines Penetrations-Tests

Ein Penetrations-Test besteht üblicherweise aus verschiedenen Teilschritten, von denen wir die wichtigsten hier in ihrer Funktion und Ausgestaltung vorstellen wollen. Es sind dies:

- der Initialworkshop
- die eigentliche Testphase
- das Verfassen des Berichts
- die Abschluss-Präsentation

3.1 Der Initialworkshop

Wichtigstes Ziel des Initialworkshops ist die Klärung und Formulierung des Erkenntnisziels des Tests. Die Beauftragung eines Pentests kann ganz unterschiedlich motiviert sein. Typische Motivationen sind beispielsweise die Überprüfung der eigenen Tätigkeit („wie gut arbeiten wir denn?"), die Überprüfung externer Dienstleister durch andere, unabhängige Dienstleister (z. B. nach einer durch den ersten vorgenommenen Firewall-Installation) oder auch nur der Wunsch, dem eigenen Streben nach Sicherheit mehr (finanzielles) Gewicht im Unternehmen zu verleihen (etwa der Geschäftsführung gegenüber).

Im ersten Fall wird der Fokus eher auf einer umfassenden Analyse liegen, ggf. unter Miteinbeziehung von Risiko-Analysen bei der Bewertung der Ergebnisse. Spektakuläre ' Hacks' wichtiger Systeme sind dann möglicherweise gar nicht gewünscht, dafür sollte aber eine Gesamtsicht möglich sein, aus der sich konkrete, umsetzbare Verbesserungsvorschläge ableiten lassen[7]. Im zweiten Fall wiederum müssen die Ergebnisse möglichst präzise und

[7] Um eine Aussage der Art „der Patch-Management-Prozess der Solaris-basierten Systeme sollte verbessert werden" zu treffen, ist es etwa bei 80 untersuchten Solaris-Systemen vielleicht nicht zwingend notwendig, auch noch den genauen openssl-Versionsstand auf den fünf nur über einen Load-Balancer erreichbaren Systemen zu ermitteln...

E. Rey et al., *Mehr IT-Sicherheit durch Pen-Tests*,
DOI 10.1007/978-3-322-80257-6_3,
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

genau verifizierbar sein,[8] und die Darstellung einer konkreten Kompromittierung könnte durchaus im Sinne des Auftraggebers sein. Im letzten genannten Fall schliesslich sollte ermittelt werden, wie tiefgehend die Ergebnisse denn sein sollen, so dass der letztliche Adressat (hier „die Geschäftsführung") nicht völlig verschreckt, aber gleichzeitig doch ausreichend verunsichert wird, um die vom Auftraggeber des Tests intendierten Massnahmen (Aufstockung des Budgets für IT-Sicherheit) zu treffen.

Von der Motivation des Auftraggebers – und damit seinem Erkenntnisziel – hängen also hochgradig die Vorgehensweise während des eigentlichen Tests und die Ausgestaltung & Formulierung des Berichts ab. Es kann auch durchaus für den Auftraggeber selbst hilfreich sein, sich das Erkenntnisziel (nochmals) klar zu machen und es zusammen mit dem Prüfer zu formulieren.

Darüber hinaus werden im Initialworkshop Ansprechpartner für verschiedene Szenarien definiert. So sollten etwa von Seiten des Auftraggebers der Datenschutzbeauftragte (zur Klärung des Umgangs mit Personen-bezogenen Daten) und ein Vertreter des Personal-/Betriebsrats anwesend sein (ein Pentest kann ja auch eine Form der Leistungskontrolle darstellen oder Ergebnisse bringen, die man in Richtung einer solchen interpretieren kann). Es müssen Ansprechpartner genannt werden für den Fall, dass es zu System- oder Netzausfällen kommt. Das gilt in beide Richtungen. Alle tatsächlichen oder vermeintlichen Störungen im Netz werden absehbar in Zusammenhang mit dem Test gebracht werden, und es ist den Sysadmins des Kunden meist sehr damit geholfen, ihnen einen Ansprechpartner zu nennen, den sie bei etwaigen Ereignissen sofort befragen können: „Haben sie gerade irgendwas gemacht, so dass der Drucker im fünften Stock nicht mehr funktioniert?".

Es müssen schliesslich – je nach Erkenntnisziel – Ansprechpartner definiert werden für den Fall, dass Sicherheitslücken gefunden werden, die so gravierend sind, dass sie im Sinne eines korrigierenden Eingriffs sofortiges Handeln erfordern. Dieser Fall gehört zu den meistdiskutierten und delikatesten Szenarien bei der Durchführung von Pentests. Streng genommen verändert ja ein Eingriff *während* des Tests das Testergebnis, was im Sinne wissenschaftlicher Arbeitsmethodik (denken Sie an die Heisenbergsche *Unschärferelation...*) oder auch der Prüf-Ethik hoch

8 Sonst wird die eigene Aussage angreifbar und damit evtl. für den Auftraggeber wertlos.

problematisch sein kann. Andererseits dient ein Test ja letztlich der Verbesserung der IT-Sicherheit (wozu ein eilig eingespielter Patch gehören *kann*), und nicht jeder Kunde hat Verständnis dafür, wenn wichtige Server „unter den Augen" und zumindest mit duldendem Wissen der „im Hause weilenden IT-Security Experten" kompromittiert werden. Das in dieser Situation richtige Handeln kann nicht eindeutig formuliert werden, und es hängt hier vom Fingerspitzen-Gefühl und der Erfahrung des Prüfers, wie er sich verhält.

Am ehesten kann die sofortige Information über eine gefundene Lücke erfolgen, wenn es sich bei Auftraggeber und „überprüftem Personenkreis" im Sinne der für die Systeme zuständigen Köpfe um dieselben Personen handelt.

Auf keinen Fall sollten Sie solche Veränderungen des Prüf-Gegenstands zulassen, wenn der Auftraggeber hierarchisch höher angesiedelt ist als der „überprüfte Personenkreis" (also das Erkenntnisziel lautet „wie gut arbeiten denn meine Admins?") oder wenn das Test-Ergebnis in offizieller Form verwertet wird (für Revisionszwecke oder zur Erlangung irgendeines Testats, das Dritten zugänglich gemacht werden soll).

Unabhängig vom konkreten Verhalten des Prüfers *müssen* im Bericht alle gefundenen Schwachstellen genannt werden, ggf. dann eben mit dem Hinweis, dass sie zum Berichts-Zeitpunkt bereits behoben sind (prüfen Sie das!). Gehen Sie weiterhin davon aus, dass Sysadmins, die schon während des Tests um Informationen bitten (um Massnahmen treffen zu können), möglicherweise ganz eigene Zwecke verfolgen und der Prüfer je nach Verhalten zum Spielball politischer Interessen werden kann. Eine gelegentliche Erinnerung an die Grundsätze der Prüf-Ethik kann in solchen Momenten nicht schaden.

Daneben werden im Zuge des Workshops, der meist ca. einen Vormittag dauert, infrastrukturelle und regulatorische Fragen (wo arbeitet der Prüfer bei internen Tests, wie erhält er welchen Zugang, welche Hallen darf er nur in Begleitung betreten, wo ist die Kantine...) geklärt.

Über alle diese notwendigen Formalia hinaus kann und sollte der Initialworkshop genutzt werden, um ein kooperatives und sachliches Klima zwischen den Beteiligten zu schaffen. Oft stehen etwa Betriebsräte Pentests sehr skeptisch gegenüber und auch eventuell anwesende Sysadmins fühlen sich häufig unwohl, in welcher Form sie denn jetzt mit möglichen und ja durchaus menschlichen Nachlässigkeiten konfrontiert werden. Ein Prüfer

hat hier Gelegenheit, klar zu machen, dass sein Anliegen keinesfalls ist, mit dem Finger auf die für gefundene Schwachstellen Verantwortlichen zu zeigen[9], sondern dass er eine wohldefinierte Prüfaufgabe zu erledigen hat, deren Ergebnis letztlich allen helfen sollte, und dies mit grösstmöglicher Sorgfalt und Unabhängigkeit zu tun gedenkt.

3.2 Die eigentliche Testphase

Ihr ist der weitaus grösste Teil des Buchs gewidmet. Daher an dieser Stelle nur die zwei Anmerkungen:

- Bedenken Sie immer das Erkenntnisziel und den möglicherweise zugrundegelegten Angreifer-Typus! Nicht immer ist der sportliche Versuch, möglichst viele Ziele (oder ein wichtiges wie einen Windows-Domänencontroller) möglichst spektakulär zu kompromittieren, im Sinne des Erkenntnisziels oder Auftraggebers. Und nicht jeder Angreifer wird grossflächig die Keule der Vulnerability Scanner anwenden. Überlegen Sie also bei der Wahl Ihrer Methoden, welche Risiken eigentlich erfasst werden sollen.
- Die wichtigsten Eigenschaften erfolgreicher Angreifer sind Ausdauer und Kreativität. Ein wenig kreatives Chaos darf durchaus zu einem Pentest gehören, und eine streng Checklisten-basierte Vorgehensweise ist nicht zwingend ein Garant für einen guten Penetrations-Test.

3.3 Der Bericht

Auch diesem Thema ist später noch ein eigenes Kapitel (Kap. 12) gewidmet.

Wir wiederholen hier deshalb nur unsere Ermahnung, das Erkenntnisziel zu bedenken und darüber hinaus den potentiellen Leser im Auge zu behalten. An vielen Stellen zu wiederholen, dass die auf den Unix-Systemen vorhandene *sendmail*-Version theoretisch für einen bestimmten Buffer Overflow anfällig ist (und unter welcher URL beim Hersteller der entsprechende Patch bezogen werden kann, der übrigens diese oder jene MD5-Prüfsumme hat), ist möglicherweise weder für den Auftraggeber – der schon lange verstanden hat, dass es Mängel beim Patch-

[9] Die sich überdies oft gar nicht exakt identifizieren lassen. Dafür sind heutige IT-Umgebungen meist zu komplex.

Management gibt – noch für die betroffenen Sysadmins (die am liebsten eine abhakbare Liste hätten, welche Systeme sie denn nun patchen sollen) hilfreich. Andererseits kann der Blickwinkel des Lesers des Berichts aber auch ausdrücklich sein, wie genau es dem Prüfer gelungen ist, exakt dieses eine System (das zufälligerweise in den Verantwortungsbereich eben dieses Lesers fällt...) zu kompromittieren, während er, der Leser, sich für alle anderen Systeme nicht interessiert[10]. Und nicht immer ist bei einem internen Test die permanente Erwähnung der vom Scanner monierten *Null Session* der Windows-Systeme sinnvoll.

Von Nutzen wäre vielmehr eine Bewertung, *warum* im gegebenen Kontext bestimmte *Findings* Probleme darstellen, oder eben auch nicht, und welche Risiken für welche Gegenstände denn eigentlich drohen. Das allerdings setzt voraus, dass der Prüfer Einsicht in die Risiko-Analysen oder die Security Policy des Auftraggebers hat, oder in die Lage versetzt wird, etwa die Geschäftsprozesse verstehen zu können, damit er zugehörige Risiken auch *bewerten* kann. Nicht jeder Auftraggeber wird jedoch solche Dokumente zur Verfügung stellen (würde sich doch sonst herausstellen, dass die seit Jahren in Arbeit befindliche Policy immer noch nicht fertig ist) oder aber bereit sein, den entsprechenden Aufwand auch zu bezahlen: „Sie (der Prüfer) sollen ja nur testen, die Risiko-Bewertung machen wir dann intern."[11].

Generell sollte der Bericht mindestens eine detaillierte Darstellung aller Ergebnisse, Tools und Methoden enthalten[12] , eine für Nicht-Techniker lesbare Zusammenfassung oder Abstraktion sowie Massnahmen-Empfehlungen samt einer Priorisierung der empfohlenen Massnahmen, ggf. unter Berücksichtigung der finanziellen, administrativen oder politischen Gegebenheiten des Auftraggebers.

---

10 Für die ja auch die Kollegen der anderen Abteilung zuständig sind, die eh' keine Ahnung haben (weshalb eine Kompromittierung natürlich zu erwarten und nur eine Frage der Zeit war...).

11 So wie die Policy... oder die Logfile-Auswertung... oder die vollständige System-Dokumentation...

12 So dass „ein sachkundiger Dritter sie in angemessener Zeit lesen und verstehen kann", um eine in der Revision oft genannte Richtlinie zu verwenden.