Ziele, Methoden und Praxis bei Penetrationstests

Die Kunst des weißen Hackens

Wer die Nachrichten aufmerksam verfolgt, der hört beinahe täglich von erfolgreichen Hackerangriffen und gestohlenen Unternehmensdaten. Jede Woche werden große Unternehmen wie Sony, LinkedIn, Blizzard, Philips und AMD Opfer von Cyberangriffen. Die Hacker finden immer wieder Schwachstellen in den IT-Systemen der Unternehmen, die sie für erfolgreiche Angriffe nutzen können. Doch warum sind Hacker so erfolgreich, und wie kann sich ein Unternehmen besser vor ihnen schützen? Penetrationstests liefern darauf die Antworten.

IT-Sicherheit lässt sich auf verschiedene Art und Weise testen. So kann zum Beispiel das IT-Sicherheitskonzept einer theoretischen Prüfung unterzogen und die Konfiguration der IT-Sicherheitssysteme kritisch betrachtet werden. Auch können Zertifizierungen umgesetzt werden, die die Einhaltung von Sicherheitsrichtlinien bestätigen. Die Liste der möglichen Testszenarien ist lang und jeder Test hilft, die IT-Sicherheit zu erhöhen und Erfolgsaussicht eines Hackers zu verringern. Doch wie sieht die Arbeit eines Hackers eigentlich aus?

Führt ein Hacker einen Angriff auf ein IT-System aus, so testet er auch dessen IT-Sicherheitsmechanismen. Es werden Informationen gesammelt, Konzepte auf Schwachstellen abgetastet und die Konfiguration der Zielsysteme überprüft. Hacker und Unternehmen testen somit zum Teil sehr ähnlich. Allerdings halten sich Hacker dabei nicht an anerkannte Testmuster und standardisierte Zertifizierungsprozesse. Sie testen auf ihre eigene kreative und unkonventionelle Art und Weise und kennen im Prinzip keine Grenzen.

Was sind Penetrationstests?

Als Penetrationstest werden Testszenarien bezeichnet, bei denen IT-Sicherheits-Experten einen Rechner oder ein Rechensystem mit den Mitteln und Methoden eines Hackers auf Schwachstellen untersuchen. Dazu beauftragen und autorisieren Unternehmen meist externe IT-Sicherheitsfirmen und erhalten von diesen gegen Bezahlung einen Bericht über die durchgeführten Tests und die dabei gefundenen Schwachstellen. Umfang, Ziele und erlaubte Testmethoden werden vorab vertraglich vereinbart und legen den Rahmen und die Ausrichtung des Penetrationstests fest. Untersucht werden zum Beispiel einzelne Programme, Webseiten, Rechnersysteme, Dienste oder Netzwerke.

Ziel eines Penetrationstests ist es, Schwachstellen und Sicherheitslücken der untersuchten IT-Systeme aufzudecken, zu bewerten und Gegenmaßnahmen zu empfehlen. Dadurch kann die Gesamtsicherheit des IT-Systems erhöht und gleichzeitig der aktuelle IT-Sicherheitsstandard des untersuchten IT-Systems dokumentiert werden.

Ablauf eines Penetrationstests

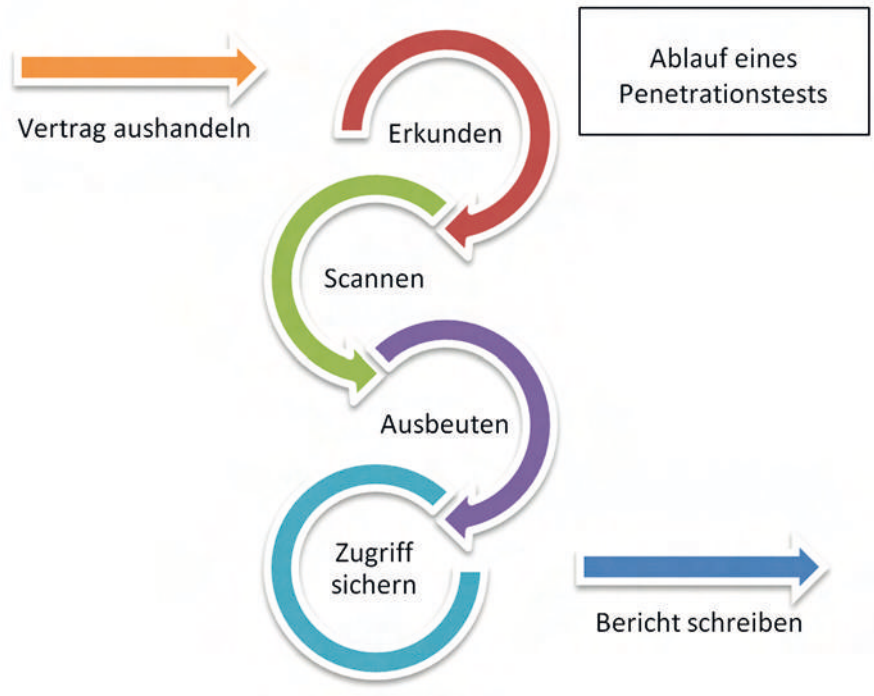
Um besonders erfolgreich sein zu können, ist es wichtig, dass ein Penetrationstest ein nur lose gegliederter Prozess ist. Wird der Penetrationstest zu stark schematisiert und an ein striktes Vorgehen geknüpft, so wird er gleichzeitig seiner kreativen und unkonventionellen Natur beraubt und verliert an Effektivität und Authentizität.

Auf neu gewonnene Erkenntnisse reagiert jeder Penetrationstester genau wie jeder Hacker unterschiedlich – entsprechend seiner Erfahrungen und Vorlieben. Der Zeitpunkt eines Informationsfundes variiert naturgemäß von Test zu Test. Würde dem Tester eine bestimmte Reaktion vorgeschrieben, so könnte es passieren, dass Schwachstellen unentdeckt bleiben, die ein Hacker durch sein ungebundenes Vorgehen sofort entdecken würde. Im weiteren Verlauf wird ein Penetrationstest in fünf lose Phasen eingeteilt, zwischen denen der Tester situationsabhängig springt. So können neue gewonnene Erkenntnisse den teilweisen Rückschritt in frühere Phasen bedingen.

Phase 0: Rechtliches Rahmenwerk

Vor Beginn des eigentlichen Penetrationstests muss ein Vertrag zwischen der testenden und der getesteten Partei ausgehandelt werden. Dieser gilt als Legitimationsbasis und unterscheidet den Penetrationstester maßgeblich von einem Hacker.

Aufgabe der Verhandlungen ist es, die Rahmenbedingungen und Ziele des Penetrati-



Ablauf eines Penetetrationstests. Quelle: ifis

onstests zu bestimmen. Der Vertrag umfasst die Angaben darüber, mit welchen Methoden welche IT-Systeme untersucht werden sollen. So gibt es neben den Zielsystemen auch „no-go"-Areas, die von den Testern auf keinen Fall penetriert werden dürfen. Dies können zum Beispiel produktionskritische oder unternehmensfremde IT-Systeme sein. Bei ihrer Auswahl sollte allerdings bedacht werden, dass kein Hacker solche Grenzen kennt und ein Penetrationstester durch sie eventuell erheblich eingeschränkt wird. Neben den vom Auftraggeber definierten „Off-limit"-Bereichen obliegt es den Penetrationstestern, auf gesetzliche Grenzen hinzuweisen.

Des Weiteren umfasst der Vertrag Angaben zur Art des Penetrationstests. So können die Tests als Black-Box-Test, das heißt ohne die Bereitstellung von zusätzlichen Informationen, oder als White-Box-Test durchgeführt werden. Bei einem White-Box-Test bekommen die Penetrationstester umfangreiche Informationen zur Verfügung gestellt und können damit den Zeitnachteil gegenüber Hackern verringern. Es können sogar Mitarbeiter des Unternehmens für kurze Zeit in das Penetrationsteam wechseln, um eine wohlinformierte Insider-Attacke nachzubilden. Als Mischform existiert der Gray-Box-Test, bei dem das Penetrationsteam nur einen Teil der Informationen erhält.

Neben gegebenenfalls ausgeschlossenen Angriffsmethoden, beispielsweise Distributed Denial of Service (DDoS)-Attacken, stellt ein Non-Disclosure Agreement (NDA) einen weiteren wichtigen Punkt der Verhandlung dar.

Letzter, aber nicht unwichtiger Aspekt der Verhandlungen ist der zeitliche und finanzielle Rahmen des Tests. Hier gilt es, das richtige Maß zu finden. Während ein kurzer und oberflächlicher Test lediglich offensichtliche Fehler finden und beseitigen kann, werden komplizierte Schwachstellen, wenn überhaupt, nur unter Einsatz von erheblichen finanziellen Mitteln aufgedeckt. Nach Abschluss dieser Vorphase und mit Unterzeichnung des Vertrags kann das Penetrationstest-Team zur vereinbarten Zeit mit den Tests beginnen.

Phase 1: Erkunden des Ziels

Am Anfang des Penetrationstests steht die Aufklärungsphase. Dabei wird nach allgemeinen Informationen zu den Zielsystemen gesucht. Dazu gehören zum einen direkte Informationen wie IP-Adressen, Dienste und Webseiten der Zielsysteme, zum anderen allgemeinere Informationen über die Unternehmen. Darunter fallen auch Informationen über die Mitarbeiter (Namen, E-Mail-Adressen, Forenbeiträge, mögliche Passwörter etc.), die Aufschluss über verwendete IT-Technologien, Passwort- und E-Mail-Adress-Schemata und Ähnliches geben. Ebenso nützlich können öffentliche Informationen wie Nachrichtenbeiträge und Stellenanzeigen sein. Denn durch all dies erhält ein Penetrationstester, ebenso wie ein Hacker, wichtige Einblicke über die verwendete IT-Technologie, Struktur und Verantwortungen der Firma.

Primäre Quellen während dieser Phase sind in der Regel Unternehmenswebseiten und das Web mit seinen vielen Informationsdiensten. Diese werden dazu mithilfe spezieller Tools oder Abfragetechniken auf Informationen untersucht. Allerdings kann auch ein freundliches Telefonat mit einem Mitarbeiter so manches Rätsel lösen.

Phase 2: Scannen der Ziele

Nachdem in der ersten Phase bereits einige Informationen über die Zielsysteme gesammelt und identifiziert wurden, besteht das Ziel der zweiten Phase darin, diese genauer zu analysieren.
Sinn dieser Untersuchung ist es, alle genutzten IP-Adressen sowie offenen Ports der adressierbaren IT-Systeme zu finden und genauer zu identifizieren (Betriebssysteme, Anwendungen … Hersteller, Versionsnummern …). Dabei werden auch mögliche IT-Schutzmaßnahmen des Unternehmens untersucht und nach Möglichkeit umgangen. Wurde beispielsweise in einem Zeitungsbericht, in einem sozialen Netz oder einer anderen öffentlichen Quelle über die Nutzung von Honeypots berichtet, so wird ein Penetrationstester versuchen, mögliche Honeypot-Server zu identifizieren und zu meiden.

Honeypot
Als Honeypot werden IT-Systeme bezeichnet, die Angreifer von ihrem eigentlichen Ziel ablenken sollen. Dabei wird ein echter Zieldienst simuliert und jede Aktion des Angreifers protokolliert. Da der Honeypot keinen echten Dienst anbietet und regulär nicht genutzt wird, kann jeder Zugriff auf den Dienst als Angriff gewertet werden. So ist es möglich, Angriffe zu erkennen und deren Verlauf zu analysieren.

Nachdem alle aktiven Dienste ausgemacht wurden, werden diese auf Schwachstellen untersucht. Dies geschieht im Zusammenspiel von automatisierten Schwachstellenscannern und der Auswertung von Schwachstellendatenbanken wie zum Beispiel der National Vulnerability Database von NIST (1).

Phase 3: Ausnutzen der Schwachstellen

In der nächsten Phase werden die gefundenen Schwachstellen nun dazu genutzt, mögliche Bedrohungen zu identifizieren. Inwieweit der Penetrationstester Sicherheitslücken dabei aktiv ausnutzt, hängt von den vertraglichen Vereinbarungen und Zielen ab. So lassen sich durch manche Schwachstellen Systemabstürze provozieren, während andere den administrativen Zugriff auf Zielsysteme erlauben. Für eine Ausnutzung der Schwachstellen kann die Verwendung eigener oder fremder Angriffsprogramme, das Eindringen in Webanwendungen durch Injections, das Mitschneiden und Auswerten von Netzwerkverkehr des Zielsystems oder das Durchführen eines Brute-Force-Angriffs gegen Login-Möglichkeiten nötig sein. Dazu steht eine buntgemischte Palette von Penetrationsprogrammen zur Verfügung, zu deren populärsten Vertretern Metasploit zählt.

Phase 4: Sichern des Zugriffs

Sollte es dem Penetrationstester gelingen, administrativen Zugang zu Zielsystemen zu erhalten, so wird dieser Zugriff nun persistiert. Dies ist nötig, da Schwachstellen oft nicht zuverlässig nutzbar sind oder durch Patches geschlossen werden könnten. Des-

wegen können beispielsweise Hintertüren in Form von Rootkits, Webshells und absichtlichen Konfigurationsfehlern in das Zielsystem installiert werden. Da dieser Schritt die Gesamtsicherheit und Stabilität der Zielsysteme negativ beeinflusst, entfällt er meist. Im Testbericht wird dann lediglich auf die Möglichkeit dieses Vorgehens hingewiesen.

Phase 5: Erstellen des Berichts

Während der eigentliche Test an dieser Stelle beendet ist und ein Hacker an seinem Ziel angekommen wäre, so gilt es für den Penetrationstester, die Daten und gefundenen Schwachstellen auszuwerten, zu sortieren und zu einem Bericht zusammenzufassen. Dieser umfasst in der Regel drei Teile: Den Anfang macht eine „Executive Summary", in der die gefundenen Schwachstellen und die sich daraus ergebenen Risiken kurz und knapp aufgeführt werden. Darauf folgt ein detaillierter technischer Bericht, mit dessen Hilfe die Schwachstellen rekonstruiert und geschlossen werden können. Den Abschluss bildet ein detailliertes Prüfprotokoll. Dieses enthält den genauen Testablauf inklusive Zeitangaben und Ausgabe der einzelnen Programme und dient als Nachweis aller getätigten Tests und Ergebnisse.

Während einige Unternehmen es bei einem einmaligen Penetrationstest belassen, ist es durchaus sinnvoll, Penetrationstests in kleinerem Umfang regelmäßig und eventuell sogar von unterschiedlichen Personen und/oder Unternehmen durchzuführen, um auf eine veränderte Sicherheitslage zu reagieren.

Der Nutzen von Penetrationstests

Natürlich liegt die Frage nach dem Nutzen nahe: Warum sollte ein Unternehmen mehrere tausend Euro in einen Penetrationstest investieren und das, nachdem ein Großteil des IT-Sicherheitsbugets bereits verplant ist? Penetrationstests helfen, Sicherheitsproblematiken zu finden, die konventionellen Tests verborgen bleiben. Selbst wenn ein Unternehmen teure und umfangreiche Sicherheitssoftware verwendet, garantiert dies alleine keine Sicherheit. Hacker können weiterhin Konfigurationsfehler oder konzeptionelle Schwächen finden. Auch resultierende Schwachstellen aus Programmierfehlern lassen sich nicht ausschließen.

Findet ein Hacker eine solche Schwachstelle, dann können die Folgekosten für das Unternehmen erheblich sein. So bezifferte Sony die Kosten des „LulzSec"-Einbruchs 2011 auf seiner Webseite mit rund 600.000 Dollar (2) und laut Steve Sordello, Chief Financial Officer von LinkedIn, zahlte das Unternehmen bis zu einer Million Dollar alleine für die forensische Untersuchung des Hackereinbruchs bei LinkedIn (3). In beiden Fällen hätte ein Penetrationstest den Erfolg des Hackerangriffs verhindern oder zumindest den Schaden deutlich senken können. Denn das Überprüfen der Webseite auf mögliche Schwachstellen, die mittels SQL-Injections ausgenutzt werden können und die kritische Begutachtung der Passwortsicherheit, gehören zum kleinen Einmaleins eines Penetrationstesters. ■

Fehlerquellen von IT-Systemen

Schwachstellen von IT-Systemen können verschiedene Fehlerquellen zugrunde liegen:

Softwarefehler:
Je komplexer eine Software ist, desto wahrscheinlicher enthält sie Fehler. Softwarefehler können zu Schwachstellen führen, die von Hackern für Angriffe genutzt werden, um IT-Systeme zu manipulieren oder lahmzulegen.

Konfigurationsfehler:
Da die Konfiguration von Software oft nicht trivial ist, kommt es zu fehlerhaften Konfigurationen. Die daraus resultierenden Schwachstellen können ebenfalls von Hackern genutzt werden.

Menschliches Versagen:
Neben fehlerhafter Software können auch Mitarbeiter, vor allem im Rahmen von Social-Engeering-Angriffen, einen Schwachpunkt darstellen. So geben sie wichtige und geheime Informationen an einen Hacker preis, während dieser ihnen ein gut inszeniertes Gaunerstück vorspielt.

Sicherheitsprobleme in der Konzernpolitik:
Fehlerhafte Policies und Verhaltensvorschriften können sich ebenfalls als Schwachstelle im System erweisen. So kann die sicherste Tür nichts ausrichten, wenn ein Besucherausweis ausreicht, um sie zu passieren. Auch wer triviale Passwörter erlaubt, handelt grob fahrlässig.

Thomas Propach,
Penetrationstester am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen

1 *http://nvd.nist.gov/*
2 *http://www.heise.de/newsticker/meldung/LulzSec-Weiterer-mutmasslicher-Sony-Hacker-in-Haft-1677798.html*
3 *http://www.zdnet.com/breach-clean-up-cost-linkedin-nearly-1-million-another-2-3-million-in-upgrades-7000002115/*