



Kosten und Nutzen von Penetrationstest

Abstract

Für kriminelle sind Unternehmensnetze ein attraktives Angriffsziel. Unternehmen schützen sich dagegen mit unterschiedlicher IT-Sicherheitstechnik. Penetrationstests sind ein probates Mittel, die Effizienz der eingesetzten IT-Sicherheit neutral zu überprüfen und Schwachstellen aufzudecken.

I.	Einleitung.....	1
II.	Kosten/Nutzen-Analyse: IT-Security	3
A.	Identifikation der passenden Budget-/Massnahmenkombination	3
B.	Penetrationstests zur Budgetfindung.....	4
III.	Der Penetrationstest	4
IV.	Penetrationstests als Prozess	5
V.	Das Spannungsfeld zwischen externer Prüfung und interner Entscheidung	5
VI.	Risiken bei Penetrationstests	5
VII.	Der Heisenberg-Effekt	6
VIII.	Ethische Aspekte bei PenTests.....	7
IX.	Rechtliche Aspekte bei Penetrationstests	7
X.	Kosten bei Penetrationstests	7

1 Einleitung

Für kriminelle Hacker¹ sind Unternehmensnetze ein attraktives Angriffsziel. Während bei einer traditionellen Straftat wie z.B. Diebstahl für den Täter ein konkretes Risiko besteht, überführt zu werden, ist dieses Risiko im Bereich der IT-Delikte nahezu null. Bei Datenspionage weiss der Geschädigte häufig selbst nichts vom Vorfall – und wird so keinerlei Ermittlungen einleiten. Die Täter sind sich dessen natürlich bewusst - und führen sorglos eine sehr grosse Anzahl von Angriffen durch (siehe [Mitnick 2003]).

Mittlerweile ist IT-Security in aller Munde: zunehmend wird sowohl Führungskräften– als auch dem Gesetzgeber klar, dass sich jedes Unternehmen in einer totalen Abhängigkeit von

¹ Der Begriff Hacker soll hier die Bedeutung einer Person haben, die sich unberechtigt Zugang zu IT-Systemen verschafft. Insbesondere im amerikanischen Sprachraum hat der Begriff noch eine weitere Bedeutung. Siehe <http://www.wikipedia.de/hacker>.

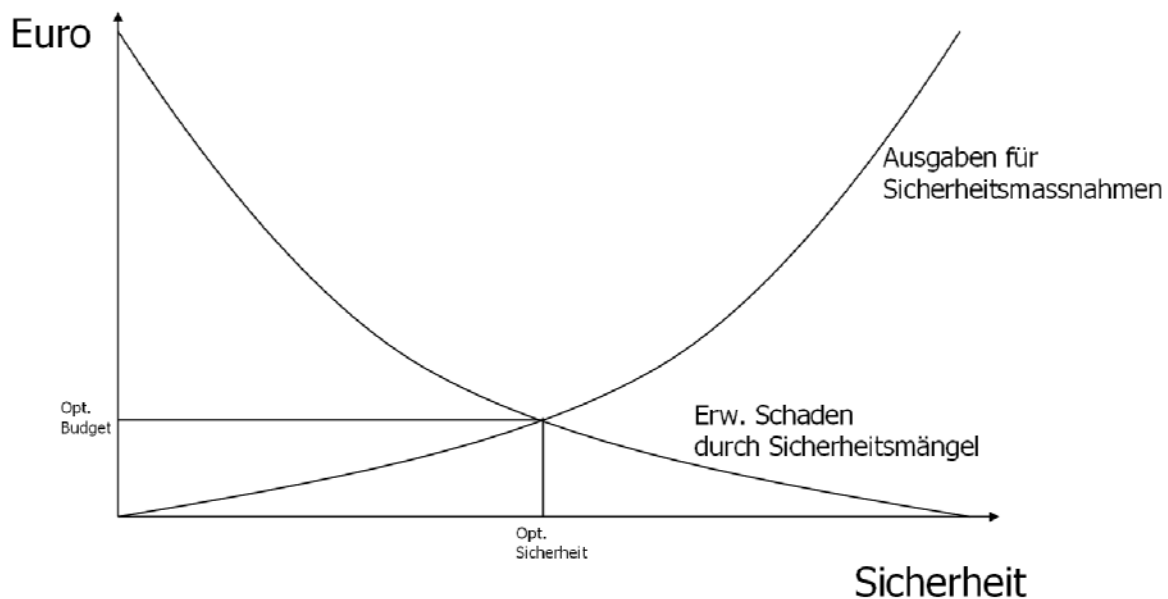
der IT befindet.

Denn der Verfügbarkeit von IT-Systemen sowie der Vertraulichkeit von Daten kommt eine besondere Bedeutung zu - der Verlust dieser Merkmale kann einem Unternehmen Schaden zufügen, der nur durch seinen eigenen Wert begrenzt ist. Damit hat man schon zwei Anforderungen an das Sicherheitsniveau definiert.

Um dieses erwünschte Sicherheitsniveau zu erreichen, muss man zunächst die Soll/Ist-Abweichung ermitteln. Es muss festgestellt werden, an welchen Stellen Massnahmen lohnend sind - und an welchen nicht.

2 Kosten/Nutzen-Analyse: IT-Security

Die Steuerung der IT-Security hat sich aber der Gewinnmaximierung eines Unternehmens unterzuordnen: es ist keine Maximierung anzustreben – sondern eine Optimierung. Das bedeutet, dass die Summe aus den Kosten für Sicherheitsmassnahmen und der durch Sicherheitsmängel entstehenden Schaden minimiert wird. Wie aus dem Schaubild ersichtlich ist, gibt es also ein Optimum an Sicherheit.



2.1 Die passende Budget-/ Massnahmenkombination

Eine scharfe, analytische Bestimmung der optimalen Budget-Massnahmenkombination ist - wie in den meisten Bereichen - auch in der IT-Security unmöglich.

Leider versagen auch heuristische Methoden, wie wir sie z.B. bei der Identifizierung von Werbebudget / Werbemassnahmen kennen. Eine Supermarktkette kann Tests durchführen indem Budget und Massnahmen-Mix regional beziehungsweise zeitlich gezielt variiert werden. Eine optimale Budget-Massnahmenkombination kann so ermittelt werden.

Solche empirischen Studien sind im Bereich der IT-Security nur schwer denkbar, da eintretende Schäden dem Geschädigten oft nicht bekannt werden. Als Beispiels hier einige Fragen:

- Ein Unternehmen betreibt eine teure, dreistufige Firewall mit IDS/IPS-Funktionalität. Würde das System durch eine einfache, Linux-basierte Firewall ersetzt werden: um wie viel Euro höher wäre der zu erwartende Schaden durch Missbrauch innerhalb eines Jahres?
- Der Vorstand eines Unternehmens kommuniziert bereits seit fünf Jahren per unverschlüsselter Email mit einer externen Rechtsanwaltskanzlei; dabei werden Vertragsentwürfe übermittelt. Wie hoch ist der daraus entstandene Schaden?
- Ein Unternehmen zieht in Erwägung, aus Kostengründen ab 2006 auf Penetrationstests zu verzichten. Von einer Verschlechterung des Sicherheitsniveaus und möglicherweise höheren Schäden wird ausgegangen. Übertrifft der Erwartungswert des zusätzlichen Schadens die Ersparnis?

Dass sich solche Fragen kaum beantworten lassen, ist systeminhärent. In der Praxis werden Budgets kaum analytisch bestimmt, man handelt pragmatisch:

- Budgetfindung nach verfügbaren Mitteln: wenn am Jahresende Budget übrig ist, wird eine Investition getätigt.
- Aktionismus: Wenn ein Schadensfall eingetreten ist, wird sehr schnell eine Investition getätigt, um zu dokumentieren, dass angemessen reagiert wurde.
- Kontinuität: Dasselbe Budget wie im letzten Jahr wird angesetzt.
- Parallelverhalten: man führt ähnliche Investitionen durch, wie andere Unternehmen (*Me-too-Effekt*)
- Externe Berater: man folgt den Vorschlägen externer Berater

2.2 Penetrationstests zur Budgetfindung

Penetrationstests entsprechen anscheinend dem letzten angeführten Punkt; allerdings werden hier dritte nicht primär beauftragt, Massnahmen zur IT-Sicherheit vorzuschlagen, sondern den aktuellen Stand neutral zu überprüfen und Schwachstellen aufzudecken. Die Konsequenzen daraus muss der Auftraggeber unter Nutzung internen Wissens und eigener Ziele selbst ziehen. Penetrationstester sollten nicht als Unternehmensberater sondern viel mehr als Prüfer betrachtet werden.

In der Praxis versuchen Unternehmen, die IT-Sicherheit durch eine Erhöhung der Budgets zu verbessern. Ursächlich für Sicherheitsprobleme sind aber in aller Regel Schwachstellen, die „einfach übersehen“ wurden. Eine leistungsfähigere Hardware löst das Problem also in keiner Weise. Ein Penetrationstest führt dazu, dass das knappe Budget viel gezielter eingesetzt werden kann und dadurch oft sogar Geld gespart werden kann.

3 Der Penetrationstest

Ein Penetrationstest ist eine Massnahme zur Ermittlung entscheidungsrelevanter Daten. Er unterstützt Entscheider dabei, festzustellen, inwiefern Unternehmensnetze angreifbar sind und ermöglicht, Investitionen viel rentabler einzusetzen (siehe [BSI 2003])

Im Rahmen des Tests führen Spezialisten gezielte Angriffe auf die IT-Infrastruktur durch. Hierbei kommen automatische Scanner, Hacker-Tools, Exploits sowie individuell erstellte Angriffswerkzeuge zum Einsatz.

Ein Penetrationstest erhebt keinen Anspruch auf Vollständigkeit, den schliesslich muss er in einem angemessenen Zeitrahmen durchgeführt werden. Es werden aber genau diejenigen Schwachstellen gefunden, die das Unternehmen am stärksten bedrohen und deren Behebung sich am meisten lohnt.

Die Motivation zur Durchführung eines Penetrationstests ist mannigfaltig:

1. Dokumentation von Schwachstellen
2. Bestandteil der Abnahme beim Projektabschluss
3. Rechtfertigung von Investitionen
4. Im Rahmen der Qualitätssicherung
5. Penetrationstests bei der Risikoinventarisierung bei KontrAG-Projekten
6. Dokumentation eines hohen Sicherheitsniveaus gegenüber Kunden und Investoren

4 Penetrationstests als Prozess

Eine einmalige Durchführung eines Penetrationstests ist nicht anzuraten: der Penetrationstest ist am sinnvollsten in einen permanenten Prozess der Qualitätssicherung einzugliedern. In der Regel wird ein Testplan für die folgenden 2 Jahre erstellt, der dann turnusmässig den aktuellen Anforderungen angepasst wird.

	Q2 2006	Q3 2006	Q4 2006	Q1 2007	Q2 2007	Q3 2007	Q4 2007
Penetrationstest auf die externen IP-Ranges		X			X		
Simulierte Angriffe gegen die Web-Applikationen			X			X	
Interner Penetrationstest				X			X
Angriffe auf die TK-Anlage	X				X		
WLAN-Screening		X				X	

Frequenz und Testtiefe werden je nach Unternehmen individuell festgelegt – und können auch situativ angepasst werden.

5 Das Spannungsfeld zwischen externer Prüfung und interner Entscheidung

Bei einer periodischen Überprüfung auf Schwachstellen hin werden die Ergebnisse des Penetrationstests nach jedem Test evaluiert und in der Regel die Probleme behoben.

Die Phase der Problembhebung besteht aber nicht aus der Durchführung von rein technischen Massnahmen sondern auch aus organisatorischen. Wird bei einem Test beispielsweise festgestellt, dass eine Gruppe von Servern erhebliche Mängel aufweist, kann die richtige Entscheidung auch darin bestehen, die Server abzuschalten oder durch Filtersysteme zu isolieren oder die Leistung der Systeme extern zuzukaufen. In die Entscheidung gehen offensichtlich interne Informationen ein, über die der Penetrationstester nicht verfügt.

6 Risiken bei Penetrationstests

Ein Penetrationstest ist eine Diagnosemethode, die Risiken in sich birgt – und muss daher von Spezialisten durchgeführt werden (siehe auch [Herzog 2005]). So können die zu prüfenden Komponenten beeinträchtigt werden. Sehr alte Systeme können bereits bei einfachen, automatisierten Scans ausfallen. Analysiert man die Anfälligkeit eines Systems auf Buffer

Overruns so sind zumindest Abstürze einzelner Prozesse zu erwarten; eine Analyse von Web-Applikationen kann den Betrieb ebenfalls stören.

Um das Risiko zu reduzieren, ist eine Selektion der Testmethoden denkbar – durch eine derartige Verringerung des Risikos sinkt allerdings aus der durch den Test erwartete Erkenntnisgewinn. Sinnvoll ist allenfalls ein Verzicht auf D.o.S.²-Attacken – oder auf bandbreitenintensive Passwortrateattacken.

Das Risiko lässt sich aber auch reduzieren, ohne die Aussagekraft des Tests zu tangieren. Folgende Vorkehrungen können getroffen werden.

- Getestet werden spezielle Test- oder Integrations-Systeme. Produktivsysteme werden nicht geprüft.
- Kritische Tests (z.B. D.o.S.-Attacken) werden auf einen Zeitraum gelegt, bei dem ein Absturz wenig Kosten verursacht (nachts oder am Wochenende)
- Um eine starke Beeinträchtigung zu vermeiden, werden nicht alle Systeme zur gleichen Zeit angegriffen.
- Um im Fall eines Absturzes schnell handeln zu können, wird der Test stundengenau angekündigt; die Systeme werden genau überwacht. Zeichnet sich eine Beeinträchtigung ab, wird der Test abgebrochen.
- Systeme, die mehr als 4 Jahre ungepatcht im Einsatz sind, werden nicht getestet. Das Risiko kann in solchen Fällen auch ohne direkten Test eingeschätzt werden.
- Sind viele Systeme nachweisbar identisch, kann mit Stichproben gearbeitet werden.

Ein weiteres Risiko ist die Ablehnung der Mitarbeiter: Zunächst ist ein Penetrationstest eine Überprüfung eines komplexen Systems. Dies geht aber auf die Leistungen einzelner zurück, so dass damit letztlich auch die Arbeit der Mitarbeiter überprüft wird. Es ist zu empfehlen, Penetrationstests nicht *aus heiterem Himmel* durchführen zu lassen; stattdessen sind die Mitarbeiter auf den Test vorzubereiten.

Das grösste Risiko bei Penetrationstests besteht darin, dass nicht korrekt vorgegangen wird. Wird ein Test nicht von absoluten Spezialisten durchgeführt, ist davon auszugehen, dass nicht alle Lücken gefunden werden. Als Konsequenz wägt sich das Unternehmen in einer nicht vorhandenen Sicherheit.

7 Der Heisenberg-Effekt

Werner Karl Heisenberg (* 5. Dezember 1901 in Würzburg; † 1. Februar 1976 in München) war einer der bedeutendsten Physiker des 20. Jahrhunderts. Er entdeckte 1927 die Heisenbergsche Unschärferelation welche besagt, dass man Ort und Impuls eines Teilchens nicht gleichzeitig beliebig genau bestimmen kann. Das bedeutet, dass die Messung selbst notwendigerweise einen Einfluss auf das Ergebnis hat.

Sehr ähnlich verhält sich dies bei der Durchführung von Penetrationstests: allein dadurch, dass Mitarbeiter und gegebenenfalls Lieferanten wissen, dass die Arbeitsqualität geprüft wird, steigt das Sicherheitsniveau (siehe [Schreiber 2003]).

² D.o.S. Denial of Service, also ein Angriff auf die Verfügbarkeit von Systemen.

8 Ethische Aspekte bei PenTests

Obwohl Penetrationstests in aller Regel bei Mitarbeitern gerne gesehen sind, werden sie oft etwas mystifiziert – das liegt sicherlich auch an dem üblichen Hacker-Cliché, dem sich die Presse immer wieder bedient. Um seriöse Penetrationstests durchzuführen, müssen einige ethische Rahmenbedingungen beachtet werden. Einen allgemein anerkannten Verhaltenskodex für Penetrationstester gibt es leider nicht.

Häufig werden Penetrationstests von Auftraggebern dazu instrumentalisiert, um eigene Ziele durchzusetzen. Um das passende Ergebnis zu erreichen, wird versucht, das Gutachten des Penetrationstesters zu beeinflussen. Schaut man hinter die Kulissen, stellt man fest, dass der Anteil der Unternehmen, die Gefälligkeitsgutachten ausstellen, erschreckend hoch ist.

Dienstleister wiederum, die Security-Lösungen vertreiben, missbrauchen Penetrationstests häufig als Vertriebsinstrument. Es besteht die Gefahr, dass Gutachten gezielt angepasst werden, um eigene Lösungen zu verkaufen. Um diese Gefahr a priori auszuschließen, sollte man ausschließlich Unternehmen mit Penetrationstests beauftragen, die keine Produkte/Lösungen/Konzepte im Bereich IT-Security anbieten.

Eine weitere Problematik ist der unangekündigte Test. Der Autor hält es für sehr bedenklich, völlig unangemeldete Tests durchzuführen. Wenigstens die Tatsache, dass Tests durchgeführt werden, sollte den betroffenen Abteilungen mitgeteilt werden – so kann z.B. auf die Erkennung eines Angriffes angemessen reagiert und die Eskalation eingeschränkt werden. Ansonsten ist immer mit einem Vertrauensverlust der betroffenen Mitarbeiter in die Auftraggeber des Tests zu rechnen.

Strenge Kontrollen und personelle Konsequenzen rufen manchmal hervor, dass Mitarbeiter eigene Fehler vertuschen – sodass die Fehler weder bekannt noch behoben werden. Es wird empfohlen, die Identifikation und Behebung von Schwachstellen in den Vordergrund zu rücken – und nicht das Auffinden des Schuldigen („Do not blame“-Paradigma). Fingerspitzengefühl ist aber auch im Umgang mit der sogenannten Hackerszene gefragt: einerseits benötigt ein Penetrationstester Informationen von Hackern – andererseits muss er selbst eine völlig integere und vertrauensvolle Person sein. Unter welchen Umständen eine Person, ein Unternehmen, eine Marke oder ein Produkt Vertrauen genießt, ist durch den Auftraggeber einzuschätzen.

9 Rechtliche Aspekte bei Penetrationstests

Eine explizite Rechtspflicht zur Durchführung von Penetrationstest besteht nicht, lässt sich aber aus einer Vielzahl von Gesetzen und Regelungen ableiten. So fordert das KontrAG, dass bedeutsame Unternehmensrisiken zu identifizieren und zu überwachen sind. Basel II macht die IT-Security kreditrelevant. Beim Abschluss von Versicherungen hat also ein professionelles Security-Management Einfluss auf die Versicherungsprämie; bei der Aufnahme von Krediten hat es Einfluss auf den zu entrichtenden Zins.

10 Kosten bei Penetrationstests

Die Kosten von einem Penetrationstest hängen von der Testbreite sowie Testtiefe ab. Unter der Testbreite versteht man die Anzahl der zu überprüfenden Systeme. Die Testtiefe sagt aus, wie intensiv die Systeme zu prüfen sind. So bewegen sich die Kosten für den Test einer Web-Applikation (siehe [Schreiber 2002c]) von ca. 3.000-12.000€. Bei einem reinen Blackbox-Test wird eine feste Anzahl von Personentagen eingekauft; die Aufgabe des Penetrationstester

besteht dann darin, in der zur Verfügung stehenden Zeitspanne so viele Schwachstellen wie möglich aufzudecken."

Literatur

- [Stoll 1998] *Stoll, C.*: Das Kuckucksei. Fischer (Tb.), Frankfurt, 1998
- [Borrmann 2003] *Borrmann, M.*: Unentdeckte Ports scannen. Network Computing 10-11/2003, S.46
- [Borrmann 2003] *Borrmann, M.*; *Schreiber, S.*: Wer zählt, gewinnt. C't 23/2003 S. 212
- [BSI 2003] *Bundesamt für Sicherheit in der Informationstechnik*: Durchführungskonzept für Penetrationstests, 2003, <http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf>, Abruf am 25.2.2004
- [Mitnick 2003] *Mitnick, K., Simon, W.*: Die Kunst der Täuschung“. Mitp-Verlag, 2003
- [Schmidt 2001] *Schmidt, J.*; *Schreiber, S.*: Gefährliche Blockade. C't 26/2001
- [Schreiber 2002b] *Schreiber, S.*: Keine harte Nuss. Notes Magazin 1/2002
- [Schreiber 2002c] *Schreiber, S.*: Virtueller Ladendiebstahl. C't 26/2002, S.92f
- [Schreiber 2003] *Schreiber, S.*: Ans Licht gebracht. Kommune21 6/2003 S.34f
- [Schreiber 2005] *Schreiber, S.*: Suchmaschinen gestütztes Hacking. <kes> 10/2005 S.6f
- [Schmundt 2005] *Hilmar Schmudt* Bezahlter Einbruch, DER SPIEGEL 9.Mai 2005
- [Herzog 2005] *Peter Herzog* OSSTMM - Open Source Security Testing Methodology Manual, <http://www.osstmm.org/>