Penetrationstests

Simulierte Hackerangriffe als Kontrollinstrument

IT-Security ist nicht nur in Großunternehmen in aller Munde, sondern wurde mittlerweile auch zu einem Top-Thema innerhalb kleinerer Firmen des Mittelstandes. Nicht zuletzt die Beschäftigung der Medien mit diesem Thema – von Gefahren durch Viren und Würmer bis hin zur großangelegten Wirtschaftsspionage – warf letztendlich auch in der Führungsriege vieler Unternehmen die Frage nach der eigenen Absicherung gegenüber derartiger Risiken auf. Eine erste Antwort auf diese Fragestellung können Penetrationstests liefern.

■ Sebastian Schreiber, Christoph Bott

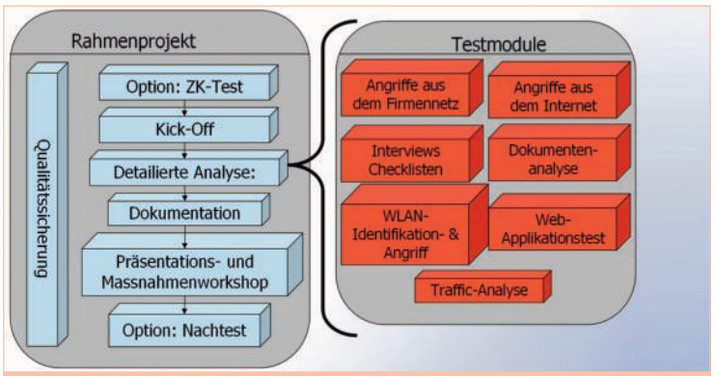
Sebastian Schreiber
ist Geschäftsführer von SySS in Tübingen
T +49/ 7071/ 40785615
F +49/ 7071/ 40785619
schreiber@syss.de

Christoph Bott
ist Security-Consultant bei SySS in Tübingen
T +49/ 7071/ 40785614
F +49/ 7071/ 40785619
bott@syss.de

In allen modernen Firmen bildet eine funktionierende IT-Infrastruktur den Grundstein für fast alle Unternehmensprozesse, im Office ebenso wie in der Produktion. Einbußen in der Verfügbarkeit von Systemen, der Integrität oder der Vertraulichkeit von Daten, führen zumeist sowohl zu unmittelbaren Auswirkungen im monetären Bereich, als auch zu teils gravierenden Ansehensverlusten. Hierdurch sind bereits die drei Hauptanforderungen bezüglich des (IT-)Sicherheitsniveaus eines Unternehmens definiert. Der Verlust nur eines dieser Merkmale kann zu unabsehbaren Schäden – bis hin zur Insolvenz – führen.

Zusätzlich bieten gerade Firmennetzwerke für kriminelle Hacker ein attraktives Angriffsziel, da im Gegensatz zu traditionellen Straftaten bei der Cyberkriminalität die Überführungswahrscheinlichkeit relativ gering erscheint. Angriffe erfolgen meist aus dem Untergrund und bleiben nicht selten unentdeckt, während gerade im Bereich der Wirtschaftsspionage veritable Profite locken.

Nicht zuletzt Neuregelungen wie KonTraG, Basel-II oder der Sarbanes-Oxley-Act führten in vielen Unternehmen zu einer Neubewertung der Frage nach dem aktuellen und dem gewünschten Sicherheitsniveau innerhalb der Unternehmens-IT. Da absolute Sicherheit nicht erreicht werden kann, steht am Anfang derartiger Überlegungen stets die Analyse des aktuellen, sowie die Definition des gewünschten Sicher-



Typischer Ablauf eines Penetrationstests. Die Testtiefe kann durch An- oder Abwahl einzelner Module einfachvariiert werden.

heitsniveaus. Durch einen Soll-/Ist-Abgleich können dann Abweichungen hiervon festgestellt und eine Kategorisierung möglicher Maßnahmen in „lohnend“ und „unrentabel“ durchgeführt werden.

Motivation

Mit Investitionen in die IT-Sicherheit verhält es sich ähnlich wie mit anderen Präventivmaßnahmen (wie etwa Versicherungsverträgen) auch: Da sich auch Vorsorgeprozesse innerhalb eines Unternehmens dem Gebot der Gewinnmaximierung zu unterwerfen haben, wird nicht ein Maximum an Sicherheit angestrebt, sondern ein betriebswirtschaftliches Optimum. Dies bedeutet, dass im Idealfall die Summe der erfolgten Aufwendungen für Sicherheitsmaßnahmen und der zu erwartenden Schäden durch Sicherheitsmängel minimiert wird.

Anders als in klassischen Bereichen der Investitionsplanung mangelt es innerhalb des Themenkomplexes „IT-Security“ an brauchbaren Kennzahlen, die für die Berechnung einer sinnvollen Budgetierung herangezogen werden können. Eine empirische Ermittlung dieser Kennzahlen ist systembedingt nicht möglich, daher folgt die Budgetplanung in vielen Fällen eher pragmatischen Ansätzen (man folgt dem, was andere vormachen; man investiert jedes Jahr die gleiche Summe) oder gar blindem Aktionismus (Investition nach Schadenseintritt). Ähnlich verhält es sich mit der Verteilung der Mittel, bei der nur allzu oft lediglich auf externe Berater oder gar schlicht auf traditionelle Verfahrensweisen vertraut wird.

Ein exaktes Risikomanagement ist aufgrund des Mangels an Kennzahlen nur schwer möglich. Penetrationstests können dieses Informationvakuum zwar nicht komplett füllen, sie liefern jedoch wertvolle Fakten über real existierende Schwachstellen in der momentanen Implementierung der Security-Policy und somit eine Entscheidungsgrundlage für die Platzierung von Investitionen. In Abgrenzung zu Unternehmensberatern im IT-Security-Umfeld obliegt es dem Penetrationstester nicht primär, Maßnahmen zur Erhöhung der IT-Sicherheit zu empfehlen, sondern den aktuellen Stand neutral und herstellerunabhängig zu bewerten um dadurch Entscheidungsgrundlagen zu liefern. Zusätzlicher Nutzen von Penetrationstests entsteht, wenn die Ergebnisse zum Beispiel in interne QA-Prozesse einbezogen werden oder aber das Sicherheitsniveau des Unternehmens gegenüber Kunden oder Investoren dokumentiert werden soll.

Durchführung

Im Rahmen eines Penetrationstests versucht der Dienstleister aus dem Blickwinkel eines potenziellen Angreifers heraus Schwachstellen in- ›

nerhalb der IT-Infrastruktur aufzufinden und auszunutzen. Für derart zielgerichtete Attacken kommen neben automatischen Scannern auch Hackertools, Exploits und selbstentwickelte Angriffsmethoden sowie persönliche Erfahrung und Kreativität zum Einsatz.

Wichtig an dieser Stelle ist, dass das Ergebnis eines Tests keinen Anspruch auf Vollständigkeit erhebt, sondern vielmehr diejenigen Schwachstellen aufdeckt, von denen die stärkste Bedrohung ausgeht und deren Behebung somit den größten Benefit verspricht. Mit welcher Testtiefe hierbei gearbeitet wird, liegt letztendlich in der Entscheidung des Auftraggebers. Maßgeblich ist an dieser Stelle das angestrebte Sicherheitsniveau einzubeziehen.

Da es sich bei einem Penetrationstest bestenfalls nicht um einen einmaligen, in sich abgeschlossenen Vorgang handelt, sondern um einen fortwährenden Prozess, womöglich im Rahmen der Qualitätssicherung, können verschiedene Aspekte der IT-Sicherheit turnusmäßig durchleuchtet werden (siehe Tabelle). In der Regel wird in diesem Fall vorab ein Testfahrplan für einen bestimmten Zeitraum erstellt, wobei Testfrequenz und Testtiefe vom Auftraggeber frei wählbar und jederzeit an aktuelle Anforderungen anpassbar sind.

Risiken und Auswirkungen

Wie jede Testmethode, die der Aufdeckung von Schwachstellen dient, birgt auch die Methodik des Penetrationstests gewisse Risiken. Daher sollten derartige Tests ausschließlich von Spezialisten mit entsprechender Erfahrung durchgeführt werden. Vor allem in produktionsrelevanten Netzen innerhalb der Fertigung sollten Tests möglichst nur an Anlagen vorgenommen werden, die nicht aktiv produzieren.

Beispielsweise kann es zu Beeinträchtigungen der Verfügbarkeit der untersuchten Komponenten kommen, insbesondere ältere Systeme können bereits bei automatisierten Scans ihren Dienst quittieren. Andere Tests führen mitunter zu Überlastungen der Netzanbindung einzelner Komponenten oder gar des gesamten Firmennetzes. Bei der Überprüfung von Anwendungen hinsichtlich Schwachstellen durch mögliche Buffer-Overflows ist wiederum mit dem Absturz zumindest einzelner Prozesse zu rechnen, während beispielsweise Tests einer Webapplikation deren Funktionalität beeinträchtigen können.

Eine Reduzierung des Risikos ist primär durch eine Beschränkung der Testtiefe möglich. Hierdurch wird allerdings ein verzerrtes Bild erzeugt, da wesentliche Aspekte unberücksichtigt bleiben und somit die gewonnene Entscheidungsgrundlage nicht auf das angestrebte Sicherheitsniveau abzielt.

Durch geschicktes Vorgehen lässt sich das Risiko eines Penetrationstest allerdings auch reduzieren, ohne das Testergebnis zu verfälschen. Folgende Vorkehrungen wären beispielsweise denkbar:

- Zeitliche Abstimmung kritischer Tests mit dem Kunden, sodass im Falle einer Betriebsstörung schnell und angemessen reagiert werden kann
- Durchführung von kritischen Tests (z.B. DoS-Attacken) in Schwachlastzeiten oder innerhalb von Wartungsfenstern
- Exemplarische Tests an Entwicklungs- oder Testsystemen anstelle der Produktivumgebung
- Bei mehreren identischen Systemen: Exemplarische Testdurchführung an nur einem System
- Reduzierung der Beeinträchtigung durch Serialisierung der Tests

Neben direkten Auswirkungen auf die IT-Infrastruktur bergen Penetrationstests allerdings auch weitere Gefahren, beispielsweise im organisatorischen Bereich. Ein derartiges Risiko könnte in der Ablehnung des Tests durch Mitarbeiter des Auftraggebers liegen, da ja letzten Endes das Ergebnis der Arbeit Einzelner überprüft wird. Daher fällt der frühzeitigen Einbeziehung der Mitarbeiter in diesen Gesamtprozess eine immense Bedeutung zu – nicht zuletzt, weil schon das frühzeitige Wissen von Mitarbeitern über die regelmäßige Durchführung von Penetrationstests dazu beitragen kann, das gesamte Sicherheitsniveau dauerhaft anzuheben.

Wichtig ist an dieser Stelle auch, dass der Penetrationstest nicht als ein ergebnisorientiertes Kontrollinstrument gesehen werden sollte, sondern als ein zielgerichtetes Werkzeug der kontinuierlichen Verbesserung. Drohen durch schlechte Testergebnisse beispielsweise personelle Konsequenzen, so steigt die Gefahr, dass Fehler vertuscht werden, wodurch wiederum das Sicherheitsniveau sinkt.

Ein weiteres Problem besteht mitunter in der Instrumentalisierung von Penetrationstests zur Erreichung persönlicher Ziele. Dies kann zum einen auf Seiten des ein oder anderen Auftraggebers beobachtet werden, wo beispielsweise versucht wird, durch direkte Einflussnahme das Ergebnis des Gutachters an das gewünschte Ergebnis „anzupassen".

Auf der anderen Seite besteht die Gefahr, dass Anbieter von Sicherheitslösungen, die selbst als Gutachter auftreten, Penetrationstests als Vertriebsmittel missbrauchen, um ihre Produkte zu platzieren.

Die wahrscheinlich größte Gefahr von Penetrationstests ist allerdings systemimmanent: Werden Sicherheitslücken, die bei der gewählten Testtiefe hätten aufgedeckt werden müssen, fälschlicherweise nicht identifiziert, so wähnt sich der Auftraggeber in einer trügerischen Sicherheit. Dieses Risiko lässt sich lediglich über die Auswahl eines kompetenten, vertrauenswürdigen Dienstleisters minimieren.

Fazit

Die Sicherheit der Unternehmens-IT – ob im Office oder im Produktionsumfeld – wird immer wichtiger. In Unternehmen, deren Geschäftsprozesse unmittelbar von der Verfügbarkeit, Integrität und Vertraulichkeit ihrer IT-Infrastruktur abhängen, stellen Penetrationstests einen wesentlichen Teil der zukunftsorientierten Unternehmensplanung dar. Richtig angewandt, helfen Penetrationstests, langfristig eine Effizienzsteigerung bei Investitionen sowie ein anerkannt hohes Sicherheitsniveau im Allgemeinen herbeizuführen und zu wahren. ■

Dieser Beitrag als PDF und weiterführende Informationen (ähnliche Beiträge, technische Daten, Direktlinks zum Hersteller etc.) sind online verfügbar auf www.SuI24.net

more @ click SI047203

Turnußmäßige Durchleuchtung verschiedener Prozesse

	Q2 2007	Q3 2007	Q4 2007	Q1 2008	Q2 2008	Q3 2008	Q4 2008
Penetrationstest auf die externen IP-Ranges		X			X		
Simulierte Angriffe gegen die Web-Applikation			X			X	
interner Penetrationstest				X			X
Angriffe auf die TK-Anlage	X				X		
WLAN-Screening		X				X	