Geleitwort zur ersten Auflage

Penetration Testing hat sich in den letzten Jahren stark etabliert: War das Thema vor einigen Jahren noch in der Domäne des Militärs und der Geheimdienste, ist Penetration Testing mittlerweile fester Bestandteil von Richtlinien wie dem Payment Card Industry Data Security Standard (PCI DSS). Die Besucherzahlen von Konferenzen wie DefCon in Las Vegas sind in den letzten Jahren explodiert. Kein Wunder, denn das Thema hat nicht nur einen gewissen technischen Sex-Appeal, sondern auch einen handfesten Nutzen. Als technischer Anwender von Metasploit haben Sie eine erfolgversprechende Zukunft vor sich: 40% der Stellenausschreibungen im Sicherheitssektor bleiben dieses Jahr wegen Fachkräftemangels unbesetzt, und Penetrationstester sind chronisch überbucht.

Ein Thema, mit dem sich viele Ihrer Kollegen – und vielleicht auch Sie – oft schwertun, ist, ein neues Sicherheitsprogramm an ein nichttechnisches Management zu verkaufen. Beide Seiten »sprechen einfach nicht dieselbe Sprache«. In diesem Geleitwort möchte ich daher versuchen zu erklären, wie Sie die Vorzüge eines Penetrationstests im Unternehmen vermitteln und dadurch benötigtes Budget sicherstellen können.

Wie sage ich es am besten?

Wir haben alle vor dem Angst, was wir nicht verstehen. Daher sollten Sie erst einmal Ihr Management mit dem Konzept eines Penetrationstests vertraut machen. Probieren Sie es einfach mit diesem Beispiel: Wir sollten uns alle in regelmäßigen Abständen einer Gesundheitsuntersuchung unterziehen, auch wenn wir uns eigentlich gesund fühlen. Nur so können schwere Erkrankungen früh erkannt und behandelt werden. Eine solche Untersuchung gehört zu den Aufgaben eines verantwortungsvollen Erwachsenen, der seine Familie und sich langfristig schützen möchte.

Dieses Beispiel lässt sich eins zu eins auf Penetrationstests anwenden, denn auch diese sollten in regelmäßigen Abständen an wichtigen Systemen durchgeführt werden. Nur so können wir erkennen, wo unsere Systeme verletzbar sind. Wir müssen diese Schwachstellen finden, bevor Kriminelle, Spione und Cyber-Vanda-

len unserem Unternehmen Schaden zufügen können. Penetrationstests gehören zu den Instrumenten einer verantwortungsvollen Unternehmensführung, die Risiken identifizieren und mindern möchte. Wie bei einer Gesundheitsuntersuchung vertrauen wir hierfür auf die Meinung ausgebildeter Experten: Ärzten und Penetration-Testern.

Aber wir haben doch eine Firewall!

»Wir haben schon so viel Geld für Sicherheitssysteme ausgegeben, und Sie sagen mir, wir wissen immer noch nicht, ob unsere Systeme sicher sind?«, mag Ihr Manager sagen. Außerdem, sollten Sie Ihre Systeme nicht gut genug kennen, um ihre Schwachstellen zu wissen? Nicht wirklich. Wenn Sie ehrlich sind, können Sie wahrscheinlich nicht einmal beschwören, dass Sie in Ihrem Unternehmen noch keine Datenpanne hatten, denn diese sind nicht immer offensichtlich.

Unsere IT-Systeme sind komplex: organisch gewachsen und mit der Außenwelt an vielen Punkten verknüpft. Es ist in vielen Netzen für einzelne Personen kaum noch möglich, einen Überblick zu behalten. Außerdem könnten Sie die intelligentesten Netzwerk-Spezialisten einstellen, und sie würden trotzdem Fehler machen. Wir brauchen also eine Art Nagelprobe, einen Realitäts-Check, eine Qualitätssicherung für unsere Netzwerksicherheit.

Der Penetrationstest stellt eine solche Qualitätssicherung dar. Sie prüft, ob all unsere Firewalls, Berechtigungssysteme, Intrusion-Detection-Systeme und Data Loss Prevention auch das tun, was wir von ihnen erwarten.

Das Geschäft mit der Angst

Vom Fahrradschloss bis zum Düsenjäger wird Sicherheit primär mit dem Angstfaktor verkauft. Bei Penetrationstests ist dies denkbar einfach: Nehmen Sie die Kosten einer Datenpanne und multiplizieren Sie diese mit der Wahrscheinlichkeit des Eintreffens in einem beliebigen Jahr. So erhalten Sie die potenziellen jährlichen Kosten mangelnder Sicherheit.

Daten hierzu gibt es zur Genüge: Das Ponemon Institute, Verizon Business, Forrester Research, und das FBI veröffentlichen hierzu regelmäßig Daten. Berechnet werden die Wahrscheinlichkeit einer Datenpanne, Kosten von Systemausfällen, der Wert gestohlener/gelöschter/manipulierter Daten, Rechtskosten und verlorener Umsatz durch Kunden, die das Unternehmen verlassen oder wegen des Vorfalls gar nicht erst zum Kunden werden. Aktuell schätzt das Ponemon Institute die Kosten pro verlorenem Kundendatensatz auf 130 Euro (145 US-Dollar). Die durchschnittlichen Kosten pro Datenpanne belaufen sich auf 3,1 Millionen Euro (3,5 Millionen US-Dollar).

Diese Zahlen sind auch sicherlich hilfreich, helfen IT-Sicherheitsfachleuten in Unternehmen aber oft nicht weiter, da die Summen so hoch sind, dass keiner sie für realistisch hält. Außerdem stammen viele der Zahlen aus den USA, wo eine Gesetzgebung, der sogenannte »Data Breach Notification Acts«, die Kosten einer Datenpanne in die Höhe getrieben hat. In Deutschland sind diese Zahlen daher, zumindest bisher, nicht direkt anwendbar. Außerdem müssen diese Zahlen den Kosten aller Sicherheitssysteme gegenübergestellt werden, nicht nur einem einzelnen Penetrationstest.

Sicherheit als Erfolgsfaktor

Penetrationstests über Angst zu verkaufen ist also möglich, aber es gibt auch andere Wege, die bei Ihrem Management eventuell besser ankommen, denn das Geschäft mit der Angst kann im Zweifel als »Erpressungsversuch« interpretiert werden. Und darauf lässt sich keine langfristige Geschäftsbeziehung aufbauen.

Penetration Testing in Kombination mit Vulnerability-Management

Eine Möglichkeit ist zum Beispiel, Penetrationstests als Kostensenker einzusetzen. Viele Unternehmen setzen bereits ein etabliertes Programm für Vulnerability-Management ein, können aber aufgrund der schieren Menge nicht alle Schwachstellen beheben. Eine Penetration-Testing-Software wie Metasploit kann in diesem Fall prüfen, welche Schwachstellen ausnutzbar sind und daher als Erstes behoben werden müssen. Durch eine solche Verfeinerung des Sicherheitsprogramms werden nicht nur die wichtigsten Schwachstellen zuerst behoben, sondern auch die Gesamtkosten für das Beseitigen von Schwachstellen gesenkt, da nicht direkt ausnutzbare Schwachstellen im ersten Schritt ignoriert werden können.

Compliance

Compliance ist oft die Brücke, über die IT-Sicherheitsfachleute mit dem Management kommunizieren können. Manager wissen, dass sie für ihren Geschäftszweig Compliance mit bestimmten Richtlinien benötigen, um Strafen zu vermeiden. Auf der anderen Seite wissen IT-Sicherheitsfachleute, dass sie über diesen Weg neues Budget beantragen können. Compliance bedeutet nicht gleich Sicherheit, aber das Compliance-Budget kann, wenn es sinnvoll eingesetzt wird, zu einer höheren Sicherheit beitragen.

Business Continuity

Viele Argumente für Penetrationstests beziehen sich darauf, was es kostet, wenn Daten gestohlen werden. Kaum eine Argumentation beleuchtet, was es bedeutet, wenn Systeme stillstehen, obwohl dies ebenfalls erhebliche Kosten verursachen

kann. Stellen Sie einfach die Frage: »Was passiert, wenn unser ERP-System eine Woche lang stillsteht?« Dieses Szenario ist für Manager wahrscheinlich deutlich greifbarer, als sich vorzustellen, was passiert, wenn die Kundendaten auf Hackerseiten verkauft werden. Auch die Kosten dürften etwas einfacher zu berechnen sein.

Unternehmensimage

Der Ruf des Unternehmens kann bei einer Datenpanne erheblichen Schaden erleiden, ist aber auch am wenigsten greifbar. Wir werden hier den Ruf des Unternehmens gleichsetzen mit seiner Marke (dem »Brand«). Besonders für Techniker ist das Konzept einer Marke nicht immer offensichtlich, daher nehmen wir einen kurzen Ausflug ins Marketingland.

Bevor wir den Schaden an einer Marke berechnen können, müssen wir uns erst einmal überlegen, wie man den Wert einer Marke berechnet: Stellen Sie sich vor, heute brennen alle Gebäude von Coca-Cola ab. Alle Fabriken, alle Abfüllanlagen, alle Verwaltungsgebäude – alles weg. Ihnen bietet jemand die Rechte an, die Marke Coca-Cola in Zukunft zu verwenden, um Getränke zu verkaufen. Was wäre Ihnen dieses Recht wert? Obwohl das gesamte Unternehmen nicht mehr existiert, hat die Marke noch einen gewissen Wert. Er ist auf jeden Fall nicht null.

Eine Marke ist ein Wiedererkennungsmerkmal für Konsumenten, um mein Produkt gegen das meines Konkurrenten abzugrenzen. Wenn ich das erste Mal in den Supermarkt gehe, um Zuckerwasser zu kaufen, habe ich ohne Marken keine Ahnung, welches ich kaufen soll. Welches schmeckt mir? Habe ich einmal »meine Marke« gefunden, kann ich sie einfach identifizieren und baue ein Vertrauensverhältnis mit ihr auf. Ich weiß, meine Marke steht für gleichbleibende Qualität und wird mich nicht enttäuschen. Sie erleichtert mir die Entscheidung beim nächsten Einkauf.

Außer über einen direkten Kontakt mit dem Produkt versuchen Unternehmen auch durch Werbung mein Vertrauensverhältnis mit der Marke aufzubauen, damit ich ihre Marke als erste ausprobiere oder von einer anderen Marke wechsle.

Viele Unternehmen investieren viel Geld für Werbung – mit steigender Tendenz, denn die Produkte in vielen Segmenten werden immer generischer. Was unterscheidet Ihr Girokonto bei der Sparkasse von dem bei der Deutschen Bank? Wahrscheinlich wenig. Falls Sie nicht Ihren besten Kumpel als Bankberater haben, war Ihre Wahrnehmung vom Unternehmen und Ihre Vertrauensbeziehung zur Marke der größte Entscheidungsträger.

Selbst bei Elektronikgeräten wird der emotionale Teil der Kaufentscheidung immer größer, da Konsumenten immer weniger zwischen den komplexen Modellen verschiedener Hersteller unterscheiden können. Wo eine rationale Entscheidung nicht mehr möglich ist, tritt eine emotionale Enscheidung an dessen Stelle, teilweise unbewusst. Dies mag für Sie als sehr technischen Penetrationstester nicht zutreffen, für das Gros der Konsumenten aber schon.

Überlegen wir uns jetzt, was passiert, wenn dieses Vertrauensverhältnis zu »meiner Marke« durch eine Datenpanne verletzt wird. Als Konsument fühlen wir uns in unserer Privatsphäre verletzt, wenn unser Online-Buchhändler die Kaufhistorie der letzten drei Jahre offenlegt. Vielleicht müssen wir sogar unsere Kreditkarte sperren lassen und haben eine Menge Scherereien. Wenn das Produkt der Konkurrenz identisch mit meinem eigenen ist, fällt die emotionale Entscheidung leicht, das Produkt zu wechseln. Dies hat direkten Einfluss auf den Umsatz des Unternehmens.

Je austauschbarer das Produkt, desto höher der Schaden. Denken wir beispielsweise an wohltätige Organisationen, würde ich wohl kaum ein zweites Mal an Brot für die Welt spenden, wenn diese meine Kreditkartendaten verschlampt haben. Dann ginge ich doch lieber zum Roten Kreuz!

Wie berechne ich einen Business Case?

Da Sie gerade ein Buch über Metasploit lesen und kein Wirtschaftsstudium absolvieren wollen, werden wir an dieser Stelle einen einfachen, pragmatischen Weg wählen. Wenn Sie tiefer in die Thematik einsteigen wollen, empfehle ich das White Paper von Marcia Wilson bei Symantec mit dem Titel »Demonstrating ROI for Penetration Testing« [1], in dem Themen wie Payback Period, Net Present Value, und Internal Rate of Return angeschnitten werden.

Für einen Business Case stellen Sie grundsätzlich zwei Dinge gegenüber: Was ist, und was könnte sein. Das »was könnte sein« ist Ihr Vorschlag. Wenn dieser Vorschlag weniger Geld kostet (oder mehr Umsatz bringt) als das, »was ist«, haben Sie einen guten Business Case. In der IT-Sicherheit lässt sich ein solcher Business Case nicht immer gut berechnen – in manchen Fällen aber schon. Wir müssen hier je nach Szenario unterscheiden.

Neue Einführung von Penetrationstests

Wenn Sie bisher keine Penetrationstests durchgeführt haben, haben Sie aktuell keine merklichen Kosten. Um einen Business Case aufzubauen, müssen Sie die Kosten einer Datenpanne oder eines Systemausfalls berechnen und diesen mit der Wahrscheinlichkeit des Eintretens multiplizieren. Hier bleibt leider nur die Angst vor einer Datenpanne als Argumentation.

Beispiel: Ihr ERP-System beinhaltet 10.000 Kundendaten. Laut The Ponemon Institute belaufen sich die Kosten pro verlorenem Datensatz auf 130 Euro (145 US-Dollar) und bei einem Gesamtschaden auf 1.300.000 Euro. Forrester schätzt, dass 60% der Unternehmen im Jahr 2015 mindestens eine Datenpanne erleiden werden, also ist die Wahrscheinlichkeit des Eintretens 60%. Der Wert des Risikos einer Datenpanne ist also 1.300.000 Euro × 60% = 780.000 Euro.

Alternativ rechnen wir aus, was der Ausfall des ERP-Systems kosten würde. Nehmen wir an, die Kosten eines Ausfalls belaufen sich auf 1 Million Euro pro Tag, und das System wäre für 3 Tage außer Gefecht gesetzt. Bei einer Eintrittswahrscheinlichkeit von 10% wären dies 3 × 1.000.000 Euro × 10% = 300.000 Euro.

Im Kontrast zu diesen potenziellen Kosten dürften Ihre geplanten Kosten für Penetrationstests recht gut aussehen. Die Frage ist, ob Ihre Berechnungen als realistisch angesehen werden.

Alternativ können Sie einfach etwas Business Jiu Jitsu anwenden, indem Sie den Penetrationstest nicht im luftleeren Raum, sondern als Teil eines Projekts unterbringen. Suchen Sie sich ein Projekt aus, das aktuell auf der Liste der Management-Ziele Ihres CIO steht. Wenn Sie die Ziele Ihres CIO nicht kennen, fragen Sie ihn einfach – und bieten Sie Ihre Hilfe an! Nehmen wir an, Ihr CIO soll in diesem Quartal 20% der externen Zulieferer per Web Services an das ERP-System anbinden. Sie können nun Ihre Hilfe für dieses Projekt anbieten und damit einen Penetrationstest in die Abnahme der Systeme einbauen. Statt nur die Web Services selbst im Penetrationstest zu prüfen, sollte selbstverständlich das gesamte ERP-System getestet werden. So werden Sie mit Ihrem Sicherheitsfachwissen zum Berater und helfen, die Technologie im Unternehmen sicher voranzutreiben.

Penetrationstests für Vulnerability-Management

Wollen Sie Penetrationstests einführen, um die Remediation-Kosten für Ihr Vulnerability-Management-Programm zu senken, sieht die Berechnung etwas anders aus:

Nehmen wir an, Sie haben drei Netzwerkadministratoren, die im Schnitt 65.000 Euro kosten. Wenn jeder dieser Mitarbeiter 20% seiner Zeit damit verbringt, Updates zu installieren und Schwachstellen zu beheben, kostet dies das Unternehmen jährlich 39.000 Euro. Wenn Penetrationstests diese Arbeit auf je 10% minimieren können, weil die Mitarbeiter nur Schwachstellen beheben, die ausnutzbar sind, spart das Unternehmen dadurch 19.500 Euro. Sie sollten außerdem in die Überlegung einbeziehen, dass die Mitarbeiter nun an Schwachstellen arbeiten, die wirklich ausnutzbar sind, und dadurch das Unternehmensnetz besser geschützt ist.

Penetrationstests intern durchführen

Wenn Sie bisher Penetrationstests durch ein externes Beratungsunternehmen haben durchführen lassen, möchten Sie diese Tests vielleicht jetzt intern durchführen und damit Geld sparen. In diesem Fall ist die Berechnung einfach, da Sie die aktuellen externen Kosten einfach den neuen internen Kosten gegenüberstellen können.

Gerade wenn Sie regelmäßig interne Penetrationstests durchführen, lohnt sich auch ein Blick auf Metasploit Pro, die kommerzielle Version von Metasploit, mit der Sie die Penetrationstests effizienter durchführen können, weniger Training benötigen und eine größere Anzahl Maschinen mit weniger Aufwand testen können.

Ziele eines Penetrationstests

Wichtig bei der Präsentation eines Business Case ist es auch, die Ziele deutlich zu kommunizieren, zum Beispiel:

- Demonstration der Verwundbarkeit der Systeme, um die Aufmerksamkeit und Unterstützung des Managements für neue Sicherheitsprogramme zu erlangen
- Senkung der Kosten eines Vulnerability-Management-Programms
- Bestandsaufnahme für neue CIOs oder CISOs
- Hilfe für Entscheidung, worauf das Sicherheitsbudget verwendet werden soll
- Testen der Response-Mechanismen von IDS-, IPS- und DLP-Systemen (Metasploit-vSploit-Module)
- Penetrationstest aus Compliance-Gründen

Fazit

Wie eine regelmäßige Gesundheitsuntersuchung gehört ein Penetrationstest zum verantwortungsvollen Verhalten eines Unternehmens. Mit der Auswahl von Metasploit als Werkzeug für dieses Unterfangen haben Sie eine hervorragende Wahl getroffen. Metasploit ist mit mehr als einer Million Downloads pro Jahr das am weitesten verbreitete Penetration-Testing-Werkzeug der Branche. Somit sind Tests mit Metasploit nahe an der Realität eines echten Angriffs.

Pentester sind aktuell sehr gefragt und werden gut bezahlt. Mit dem Spezialwissen über Metasploit, das Sie sich mit diesem Buch aneignen, werden Sie Ihren persönlichen Wert am Arbeitsmarkt nachhaltig steigern. Wichtig ist aber in jedem Fall ein solides Fachwissen, damit Sie mit dem Penetrationstest keine Systemabstürze oder Netzwerküberlastungen erzeugen.

Sollten Sie Penetrationstests zu Ihrer Haupttätigkeit machen, können Sie Ihr erworbenes Wissen auch in den kommerziellen Versionen von Metasploit weiter nutzen, die Ihnen durch Automatisierungen und Teamkollaboration ein effizienteres Arbeiten ermöglichen und dröge Aufgaben wie Beweismittelsicherung und Berichteschreiben weitgehend abnehmen.

In jedem Fall sollten Sie in Ihrem Unternehmen daran mitarbeiten, Penetration Tests in den Sicherheits-Lebenszyklus zu integrieren, so dass kein neues System ohne Penetrationstest in Produktion geht. Wenn Ihre Kollegen fragen, wann sie einen Penetrationstest durchführen sollten, antworten Sie einfach: »Wann sollten Sie im Auto einen Sicherheitsgurt anlegen?« Immer.

Christian Kirsch[1]

1 Christian Kirsch war Principal Product Marketing Manager bei Rapid7, der Firma, die seit 2009 für die Entwicklung des Metasploit-Framework verantwort-lich ist.