# Pentest 2010

## Was bringt die Zukunft für Penetrationstests?

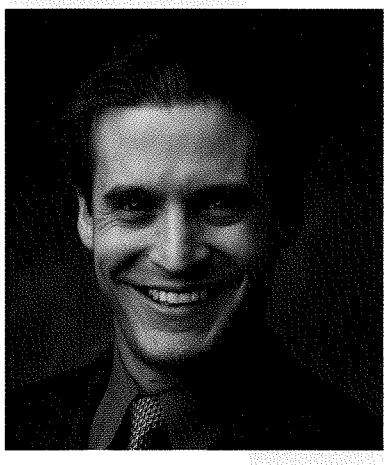
These:

# Der Pentest ist tot – lang lebe der Pentest!

*Von Brian Chess, London*

Seit Ende letzten Jahres verkünde ich freimütig meine Überzeugung, dass 2009 als Todesjahr des Penetrationstests wie wir ihn kennen und lieben in die IT-Geschichte eingehen wird. Dabei hatte ich weder zu viel Sherry über die Feiertage noch bewirkte die nüchterne Sicht des neuen Jahres einen Sinneswandel. Natürlich werden Pentester auch dieses Jahr nicht von jetzt auf gleich von der Erdoberfläche verschwinden! Pentests werden aber sehr wohl eine deutliche Transformation erfahren und letztlich als Teil eines strikt integrierten Sicherheits-Ansatzes quasi „neu geboren".

Ich halte es für unumstößlich, dass jeder Probleme bekommt, der sich nicht um die Sicherheit kümmert – und aus genau diesem Grund haben Penetrationstests eine bedeutende Rolle in Sachen Softwaresicherheit erlangt. Wie war es denn lange Zeit? Viele haben Code programmiert, von dem schnell klar war, dass er vermutlich unsicher sein würde – kaum fertiggestellt wurde das Ergebnis daher Penetrationstests unterzogen, um diese These zu untermauern. Und für dieses fundierte Wissen hat man auch noch bereitwillig bezahlt. Ich bin längst nicht mehr der Einzige, der die Sinnlosigkeit in solchem Handeln erkennt!



*Brian Chess (Fortify): „Penetrationstests werden 2009 einen grundlegenden Wandel erfahren!"*

Während verschiedener Gespräche mit Führungskräften aus großen Software-Security-Projekten hat es 2008 wenig überrascht zu hören, dass alle früher oder später auch mit Penetrationstests (meist durch externe Firmen) gearbeitet haben. Schließlich gibt es kaum ein besseres Mittel als einen brandheißen Pentest-Report, um jemanden zum Eingeständnis von Problemen zu bewegen! Dennoch: Mit der Umsetzung von Sicherheitsdenken an einem früheren Punkt im Software-Entwicklungszyklus verlieren Pentests einiges von ihrem Glanz – bekommt man die Software-Sicherheit besser in den Griff, lässt die Bedeutung von Pentests nach (bleibt aber „größer Null").

Als Aha-Erlebnis blieb: Wo Unternehmen von vornherein bessere Softwaresicherheit verwirklichen, schwindet die Besessenheit, mit Pentests Löcher nachzuweisen, von denen ohnehin klar ist, dass es sie gibt. In diesem Umfeld werden Penetrationstests dann zum Teil eines erheblich umfassenderen Ansatzes zur Verbesserung der Sicherheit – idealerweise erreicht man ein ausgewogenes Verhältnis des „Yin und Yang" von Angriff und Verteidigung.

## Wendepunkt 2008

Man gibt mittlerweile mehr Geld dafür aus, von Anfang an korrekten Code zu entwickeln, statt anschließend dessen Fehlerhaftigkeit zu beweisen. Das bedeutet zwar nicht das „Ende der Welt" für Penetrationstests (sollte es auch nicht!), aber es verändert doch einiges: Statt weiterhin ein selbstständiges „Produkt" zu sein, werden Pentests eher zur speziellen „Funktion" eines umfassenderen Produkts – der eigenständige Pentest verschwindet und wird fortan Teil einer ganzheitlichen Sicherheitslösung.

So etwas passiert übrigens ständig im Hightech-Dschungel: So waren die ersten Rechtschreibkorrekturprogramme noch eigenständige Software – sobald diese Funktion Teil jeder Textverarbeitung war, gab es für diese Dinosaurier aber keinen Markt mehr. Heute haben wir praktisch überall Rechtschreibhilfen (sogar in Programmier-Tools), aber es gibt weder Boxen mit Standalone-Korrektursoftware für PCs noch entsprechende iPhone- oder Web-2.0-Angebote – q.e.d.!

Aber warum jetzt? Die Zeit ist reif! 2007 hat IBM ein Unternehmen namens WatchFire gekauft, Hewlett-Packard akquirierte SPI Dynamics – beide übernommenen Firmen produzierten Pentest-Tools für Webanwendungen. IBM und HP haben substanzielle Beträge dafür ausgegeben – zwar keine durchgeknallten „Dotcom"-Preise, aber selbst bei HP oder IBM braucht man einen guten Grund, um über 70 Millionen Dollar lockerzumachen. Dieser gute Grund war, dass die akquirierte Technologie im Zusammenspiel mit anderen Produkten und Dienstleistungen einen guten Einstieg in den schnell wachsenden Software-Security-Markt bedeutet. Jede Übernahme will erst einmal verdaut sein – doch mittlerweile ist genug Zeit vergangen: 2009 wird das Jahr sein, in dem diese

**Veränderung oder Beständigkeit – an dieser Frage scheiden sich bei Penetrationstests die Geister von zwei Experten. Für die <kes> haben Brian Chess und Sebastian Schreiber ihre Sicht der Dinge niedergeschrieben.**

Antithese:

# Totgesagte leben länger

*Von Sebastian Schreiber, Tübingen*

„Konvergenz-Strategie" aufgeht, und im Rückblick wird 2009 das Jahr sein, in dem der größere Teil der Welt anfing, Pentests als Teil eines größeren Ganzen zu sehen.

## Anpassen oder Aussterben!

Es wird wohl immer „Security-Consulting-Boutiquen" mit lustigen Namen und exotischen Angeboten geben – aber die Security-Industrie entwickelt sich hin zu „integralem Yin und Yang". Einen Vorgeschmack hierauf liefert schon die Integration von Methoden des White-Hat-Hackings in Web-Application-Firewalls (WAF) – hier zeigt sich bereits das kreative Zusammenspiel von Angriff und Verteidigung.

Die Herausforderungen der Software-Sicherheit sind heute präsenter denn je – und Penetrationstests verdienen Anerkennung dafür, dass sie bei der Bewusstseinsbildung geholfen haben. Aber von der Existenz eines Sicherheitsproblems zu wissen, heißt noch nicht, ein Gegenmittel zu kennen – anders ausgedrückt: Pentests helfen beim Aufspüren von Problemen, aber nicht bei deren Lösung. Und genau deshalb müssen Pentester einen langen, kritischen Blick auf sich selbst richten und dann etwas verändern. Genau wie die ehrwürdigen Spell-Checker werden Pentests als solche eingehen und in einer weniger singulären, dafür aber weiter verbreiteten Form wieder auferstehen – ich zumindest kanns gar nicht erwarten! ■

*Brian Chess ist Mitbegründer und Chief Scientist von Fortify Software Inc. (www.fortify.com).*

Als ich Brian Chess' heroisch-pathetischen Ausruf „Der Pentest ist tot – lang lebe der Pentest" zum ersten Mal vernahm, kam mir eine herrlich hämische Wilhelm-Busch-Geschichte in den Sinn: Darin veranstaltet der vermeintlich frisch gebackene Witwer Sauerbrot ein Fest und trinkt darauf, dass die elende Zeit seiner Ehe nun vorbei sei – doch während sich Sauerbrot in neuer Freiheit wähnt, tritt im Laufe des Gelages die Totgeglaubte durch die Türe und Sauerbrot erstarrt vor Schreck und stirbt. Auch beim Pentest erfreut sich der Totgesagte momentan bester Gesundheit und ist so stark wie nie zuvor! Es gibt keine Anzeichen für einen baldigen Tod oder eine aussichtsreiche Alternative.

Um Zukunftsprognosen machen zu können, ist es wichtig, die Entwicklungen in der Vergangenheit zu beleuchten. Einfachen, mittelfristigen Prognosesystemen liegt die Kontinuitätshypothese zugrunde: Man geht davon aus, dass sich vergangene Entwicklungen in ähnlicher Weise fortsetzen und projiziert Vergangenheitsdaten in die Zukunft. Beobachtet man, dass der Meeresspiegel der Nordsee in den letzten 150 Jahren um jeweils zwei Zentimeter pro Jahrzehnt gestiegen ist, so lässt sich daraus schließen, dass diese Entwicklung in naher Zukunft anhalten wird.

Der Markt für Penetrationstests zeigt seit elf Jahren kontinuierlich ein starkes Wachstum. In gleicher Weise wie die Entwicklung von IT-Systemen stetig vorangetrieben wird, steigt auch das Angriffspotenzial durch böswillige Hacker, die beim Finden von Sicherheitslücken immer raffinierter werden. Es ist auch kein Trend zu erkennen, dass bei Penetrationstests im Jahre 2009 weniger Systeme geknackt werden könnten.

## Unbesiegte Featuritis

Im Gegenteil: Die Entwicklung neuer Software richtet sich (immer noch) eher *gegen* ein Mehr an Sicherheit, denn der Markt der Software-Entwicklung orientiert sich an anderen Maßstäben. Getrieben durch den Konkurrenzdruck und den Willen als Unternehmen zu überleben, sind Entwickler heute vor allem damit befasst, Software zu konzipieren, die sich auf dem Markt durchsetzen kann. Die Entwicklung muss zudem schnell gehen, damit das Produkt zügig auf den Markt kommt und Umsatz bringt. Dabei bleibt oft keine Zeit für eingehende Sicherheitsüberprüfungen. Gleichzeitig steigt die Komplexität der IT seit über 50 Jahren – eine Wende in die entgegengesetzte Richtung sehe ich nicht.

*Sebastian Schreiber (SySS): „Ich wette eine Flasche Sherry, dass der Penetrationstest nicht stirbt – im Gegenteil: Er wird innerhalb der nächsten 10 Jahre weiter an Bedeutung gewinnen."*

Nicht zuletzt bauen zudem die meisten Software-Designer auf Bestehendem auf, sodass neue Software in vielen Fällen dieselben Sicherheitslücken aufweist wie vorangegangene Versionen. Trotz des stetigen Wandels ist dies ein Beleg für die Kontinuitätshypothese, die sich eben nicht radikal durchbrechen lässt! Obschon es denkbar – und wünschenswert – wäre, dass IT-Systeme und Software in Zukunft einfacher, stabiler und sicherer werden und auch alternative Methoden der Qualitätssicherung die des klassischen Penetrationstests ersetzen könnten – die Praxis kennt keinen solchen Trend, im Gegenteil: Systeme stürzen weiter ab und verhalten sich oft ungewöhnlich. Es vergeht kaum ein Tag, an dem wir der Presse keine Berichte über Hackerattacken und Datenklau entnehmen können. Wobei das, was ans Tageslicht dringt, weiterhin nur die Spitze des Eisbergs ist – die meisten Angriffe bleiben unbemerkt oder werden vertuscht, um Skandale zu vermeiden.

## Kraft der Andersartigkeit

Es gibt etliche Standards und Prozesse, die dafür sorgen sollen, dass IT-Systeme sauber und stabil laufen: ISO 9000, ISO 27001, Grundschutz, ITIL et cetera. Checklisten und Maßnahmenkataloge für Secure-Software-Engineering sind vorhanden und im Einsatz. Dennoch geht der Penetrationstest einen anderen Weg, der sich orthogonal zu diesen Maßnahmen zeigt: Hier wird bewusst nach neuartigen Schwächen, nicht bedachten Angriffspfaden und übersehenen Schlupflöchern gesucht.



Albert Einstein sagte einmal, dass sich komplexe Probleme nicht mit demselben Denken lösen lassen, das sie geschaffen hat. Daher ist auch klar, dass die kreative Kraft, die etwas nach bestem Können entwirft, nicht gleichzeitig etwaige Schwächen in ihrer eigenen Konzeption wahrnehmen kann. Sicherheitsprobleme kann man *nicht* mit denselben Methoden finden, die zu ihnen geführt haben! Hier ist ein „Andersdenkender" gefragt, ein Advocatus Diaboli, jemand der den Blick von außen hat und mit Erfahrung, Witz, Verstand und (andersartiger) Kreativität nach bisher unbemerkten Lücken sucht. Ein beauftragter Penetrationstester ist ein solcher Advokat, der den Entwicklern seine externen Erkenntnisse zur Verfügung stellt, damit intern Sicherheitslücken geschlossen werden können, bevor der wahre „Advokat des Teufels" in Form eines böswilligen Hackers zuschlägt und ein zigfaches von dem an Schaden anrichtet, was ein externer Sicherheitstest je kosten würde.

Solche Qualitätssicherungsmethoden von außen ins Innere zu verlagern, wäre in etwa so, als würde die Wirtschaft fordern, externe Wirtschafts- und Steuerprüfer abzuschaffen, da jedes Unternehmen ja eine eigene Buchhaltung habe und ohnehin ökonomische Grundprinzipien in ihre Geschäftsprozesse integriere. Dennoch ist das Instrument der äußeren Kontrolle – wenngleich oft unangenehm – sehr wichtig, um die Qualität des Wirtschaftens zu erhalten!

Nicht anders ist es in der IT-Branche, wo Verbesserungen auch nur möglich sind, wenn Entwickler und externe Penetrationstester sich die Hand reichen. In diesem Zusammenwirken liegt das wahre „Yin und Yang" als der zu schaffende Ausgleich zwischen Angriffsmöglichkeit und Abwehr!

## Wetten dass?!

Wo Brian Chess den Tod des bisherigen Pene-trationstests voraussagt und ihn bereits für das Jahr 2009 prophezeit, möchte ich entgegnen: Ich bin überzeugt davon, dass dem Totgesagten noch viele glückliche Lebensjahre beschieden sind! Darauf wette ich gerne eine Flasche Sherry! Ob die Wette angenommen wird oder nicht: Auf alle Fälle freue ich mich schon jetzt darauf, die Flasche am Ende der nächsten Dekade zu öffnen, mir ein Gläschen einzuschenken und einen Toast auf das lange Leben des längst Totgesagten auszusprechen. ■

*Sebastian Schreiber ist Gründer und Geschäftsführer der SySS GmbH (www.syss.de).*