Penetrationstest – geschnitten oder am Stück?

Tobias Glemser, secuvera GmbH

Der Wissensstand und entsprechend die Planungen und Anfragen zu Penetrationstests sind sehr unterschiedlich. Der Artikel gibt einen Überblick darüber, was ein Penetrationstest sein kann, welche Fähigkeiten Penetrationstester haben sollten und nach welchen Standards vorgegangen wird.

Die Anfragen für Penetrationstests sind häufig sehr unterschiedlich. Dies hängt direkt mit dem Wissensstand der Fachseite zusammen, die diese Anfragen formuliert. Es ist nicht unüblich, dass die Anfrage alleinig darin besteht zu erfahren, was denn ein Penetrationstest kostet. Unter Penetrationstests kann man sehr viele unterschiedliche Prüfungen subsumieren. Dafür ist auf Seiten des Anfragenden eine gewisse Expertise notwendig. In einigen Fällen ist die Anfrage deutlich zu unspezifisch oder gar widersprüchlich.

Ein Beispiel aus der Praxis: Angefragt wird die Prüfung von Servern und Infrastruktur. In der detaillierten Leistungsbeschreibung sind dann Adressen von Web-Anwendungen genannt. Damit ist der Fokus der Prüfungen nicht klar.

Sofern es wirklich um die Prüfung von Servern und Infrastruktur, wie zum Beispiel die eines Firewall-Systems, gehen soll, ist die Vorgehensweise eine andere als bei der Prüfung von Web-Anwendungen. Es handelt sich in beiden Fällen um Penetrationstests; die Prüfmethodik ist jedoch eine andere. Aus der Prüfmethode ergeben sich auch andere Prüfrisiken.

In anderen Fällen haben sich die Ausschreibenden bereits mit dem Thema beschäftigt, Literatur gelesen und spezifizieren den Penetrationstest sehr genau. Aufgrund mangelnder Praxiserfahrung werden jedoch häufig Anforderungen gestellt, die entweder einen großen Aufwand bei geringem Erkenntnisgewinn verursachen würden oder für das jeweilige Prüfobjekt nicht zielführend sind. Darüber hinaus wird das Risiko, das von den Prüfungen ausgeht, nur selten betrachtet.

Basisprüfungen von Systemen sind vergleichsweise risikoarm. Prüfungen von Anwendungen, insbesondere auf Produktivsystemen, bergen je nach Anwendung große Risiken – beispielsweise die Veränderung von Daten, Integritätsverlust oder auch der Ausfall von Anwendungen, selbst wenn der Ausfall durch sogenannte Denial-of-Service-Angriffe (DoS) nicht explizit provoziert wird.

Definition Penetrationstests

Es gibt sehr viele unterschiedliche Definitionen von Penetrationstests. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert in seiner Studie *(siehe „https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_htm.html")* einen Penetrationstest als kontrollierten Eindringversuch, der vergleichbar zu einem realen Angriff durchgeführt wird. Er ist zeitlich begrenzt und auch nur eingeschränkt standardisierbar. Das National Institute of Standards and Technology (NIST) schreibt im Dokument SP800 *(siehe „http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf"),* dass das Ziel eines Penetrationstests ist, Schwachstellen aufzudecken. Ein Penetrationstest sei eine Resilienzprüfung vor dem Hintergrund von Zeit, Ressourcen und Kenntnissen. Ebenso wie das BSI schreibt das NIST, dass ein Penetrationstest vergleichbar mit einem realen Angriff sein soll. Damit wird klar, dass der angenommene Angreifer selbst zu definieren ist.

Welche Eigenschaften ein Penetrationstester mitbringen soll, beschreiben BSI und NIST ebenso. Ein Penetrationstester benötigt demnach langjährige Erfahrung als System- und Netzwerk-Administrator, er beherrscht Programmiersprachen, kennt sich in Produkten wie Firewalls sowie in Intrusion-Detection-Systemen aus und kennt seine Angriffswerkzeuge aus dem Effeff. Darüber hinaus ist er ein kreativer Geist. Salopp gesagt: Wenn irgendwo ein Administrator oder ein Entwickler fehlt, wie schön, dass ein Penetrationstester das alles kann. Das NIST greift einen weiteren interessanten Punkt auf: Kommunikationsfähigkeit.

Das Ergebnis eines Penetrationstests ist immer die Dokumentation des Tests. Sie muss den Leser fachlich dort abholen, wo er steht. Diese Transferleistung in einem geschriebenen Dokument muss der Penetrationstester erbringen. Insbesondere bei der Zusammenfassung für das Management ist dies enorm wichtig. Der Entscheider muss in der Lage sein, das durch die Prüfungen aufgedeckte Risiko aufgrund der Dokumentation zu bewerten. Sollen alle oder nur einige der identifizierten Schwachstellen behoben werden? Dies liegt nicht zuletzt an der Kommunikationsfähigkeit des Prüfers.

Versucht man alle Definitionen auf eine möglichst allgemeingültige und prägnante Definition zu verkürzen, so kann man formulieren: „Ein Experte führt für einen Zeitraum X einen Angriff gegen Ziel Y nach Vorgehensmodell Z durch." Letztlich wird das Risikoprofil des Angreifers abgebildet, den man simulieren möchte. Wie viel Zeit wird der Angreifer sich mit einem Ziel auseinandersetzen? Welche Expertise hat der Angreifer?

Es macht einen erheblichen Unterschied, ob man beispielsweise für die Prüfung einer Anwendung nur wenige Stunden zur Verfügung hat oder mehrere Tage. In wenigen Stunden ist selbst bei einfachen Anwendungen keine baldige Prüfaussage möglich. Bei systembasierten Prüfungen hingegen, bei denen also je System auf erreichbare Dienste und bekannte Schwachstellen innerhalb dieser Dienste geprüft wird, ist der manuelle Prüfaufwand vergleichsweise gering. Die geprüften Protokolle und Dienste sind stark automatisiert prüfbar. Dennoch gibt es von den Prüfwerkzeugen erkannte Schwachstellen, die aufgrund falscher Indizien identifiziert wurden, sogenannte „False-Positives". Diese muss der Prüfer selbstverständlich durch manuelle Verifikation der Schwachstellen identifizieren. Darüber hinaus gibt es einige wenige rein manuell durchführbare Prüfungen. Bei der Prüfung von Anwendungen oder auch bei der Prüfung von individuellen Lösungen wie etwa speziellen Produkten mit speziellen Produkteigenschaften ist die Anforderung an die Expertise des Prüfers ungleich höher.

Nutzen von Penetrationstests

Ein Penetrationstest ist im Regelfall keine deterministische Vorgehensweise. Insbesondere, da der Faktor Zeit und die Aufteilung der Zeit eine wichtige Rolle spielen. Meist werden Penetrationstests zum Festpreis durchgeführt. Dabei steht die zur Verfügung stehende Zeit im Vorfeld fest. Welchen Anteil der Projektzeit reine Prüfzeit darstellt, ist im Vorfeld für keine Partei abschließend vorhersehbar. Die Prüfzeit besteht aus den eigentlichen Prüfungen, aber auch der Lösung bei Prüfproblemen. So kommt es in der Prüfpraxis regelmäßig vor, dass Systeme und Anwendungen während der Prüfung verlangsamt antworten oder ganz abstürzen. Dies alles geht auf das Projektkontingent.

Ebenso unklar ist im Vorfeld, wie viel Zeit für die Dokumentation der Ergebnisse notwendig sein wird. Je mehr Schwachstellen während eines Tests gefunden werden, desto mehr Zeit benötigt der Prüfer für die Dokumentation. Dieses Mehr an Zeit für die Dokumentation im Falle vieler Schwachstellen geht von der effektiven Prüfzeit innerhalb des Gesamtkontingents ab. So kann es Fälle geben, bei denen durch Testabbrüche und eine Vielzahl von Anwendungen die angestrebte Prüftiefe in einem Projekt nicht erreicht werden kann. Dies ist jedoch klar zu dokumentieren. In einem solchen Fall ist die nicht erreichte Prüftiefe kein Praxisproblem. Es ist offensichtlich, dass das Prüfobjekt erheblich und grundsätzlich verbessert werden muss.

Da kann man im Regelfall von „Time Boxed"-Prüfungen sprechen. Der Tester hat eine gewisse Zeit für Prüfung und Dokumentation zur Verfügung. Der Nutzen eines Penetrationstests hängt also klar von der Expertise des Testers und der Aufbereitung des Ergebnisses ab.

Etablierte Prüfstandards

Eine grundsätzliche Definition für Penetrationstests stellt das Durchführungskonzept des BSI dar. Für spezifische Prüffälle bietet beispielsweise das Open Web Application Security Project, bekannt durch die zehn häufigsten Risiken in Web-Anwendungen (OWASP Top 10, *siehe „https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project"),* mit dem OWASP Testing Guide *(siehe „https://www.owasp.org/index.php/Testing_Guide")* eine hervorragende Möglichkeit, einen granularen Prüfplan und damit auch Prüfnachweis bei der Prüfung von Web-Anwendungen zu pflegen.

Im Rahmen des Angebots muss der Anbieter darstellen, mit welcher Methodik und welchen Werkzeugen er die jeweiligen Prüfungen durchführen möchte. Für die allermeisten Prüffelder gibt es mittlerweile spezialisierte Werkzeuge. Die Transparenz ist dabei ein hohes Gut. Nur wenn Tests nachvollziehbar sind, entfalten sie einen Mehrwert. Sicherheit und auch Penetrationstests sind kein Voodoo.

Anbieterqualifizierung

Es gibt wenige Möglichkeiten, die Qualifikation eines Anbieters zu prüfen. Ausschreibende Stellen sollten sich vorab einige Mitarbeiterprofile des Anbieters geben lassen. Deren Expertise sollte die Anforderungen abbilden. Im Falle, dass andere Personen als die angebotenen eingesetzt werden, sollte der Ausschreibende sich ein Vetorecht einräumen.

Ein wichtiger Aspekt bei der Qualifikation von Prüfern sind die Berufserfahrung, die Erfahrung in der spezifischen Prüfdomäne und personenbezogene Zertifizierungen. So gibt es zum Beispiel in Deutschland durch das BSI zertifizierte IT-Dienstleister für Penetrationstests *(siehe „https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/IS_REV_PEN/IS_REV_Dienstleister/IS_REV_Dienstleister_node.html").* Diese beschäftigen entsprechend durch das BSI geprüfte und zertifizierte Penetrationstester *(siehe „https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/PEN/personen_auditoren_pentester.html").*

Das BSI als Behörde ist wirtschaftlich unabhängig in seinen Feststellungen und führt selbst Penetrationstests für Bundesbehörden durch. Die Wertigkeit des Zertifikats ist entsprechend hoch. Es gibt weitere personenbezogene, kommerzielle Prüfungen, etwa Offensive Security Certified Professional (OSCP, *siehe „https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional")* oder der deutlich theoretische Certified Ethical Hacker (CEH, *siehe „https://www.eccouncil.org/programs/certified-ethical-hacker-ceh").*

Darüber hinaus empfiehlt es sich, Referenzen zu prüfen. Es ist zwar schwer, Referenzen in diesem Segment zu erhalten; doch für Unternehmen, die sich lange genug erfolgreich am Markt positioniert haben, sollten Referenznennungen kein Problem darstellen.

Herausforderung spezieller Prüfungen

Es ist nicht unüblich, dass sehr spezielle Umgebungen überprüft werden müssen. Das können zum Beispiel Automatisierungsumgebungen, Radarnetze oder Produktklassen wie Geldspielgeräte sein. Im Gegensatz zu Standardprüfungen, wie der Prüfung von Webshops, gibt es hier im seltensten Fall eine spezialisierte, standardisierte und etablierte Vorgehensweise. Daher empfiehlt es sich, mit wenigen grundsätzlich qualifizierten Anbietern entsprechende Workshops vorab abzuhalten. Dabei werden durch den Ausschreibenden die Prüfziele vorgestellt. Der Anbieter hat dann die Möglichkeit, spezifische Fragen zu stellen und mögliche Prüfungen aus den Angaben abzuleiten. In diesen Gesprächen ist meist relativ klar erkennbar, welche Anbieter für diese Art von Spezialprüfungen besonders geeignet sind.

Oder doch lieber ein Audit?

Es kommt in der Praxis immer wieder vor, dass Organisationen Penetrationstests planen, jedoch das zu betrachtende Risikoprofil eigentlich eher für ein Audit geeignet ist. Bei einem Audit werden zum Beispiel auf Basis der Grundschutzkataloge des BSI Grundsätze der technischen Implementierung und der Prozesse im Unternehmen abgefragt. Für kleinere Unternehmen ist der Cyber-Sicherheits-Check von ISACA und BSI eine sehr effiziente und kostengünstige Möglichkeit, eine Bewertung der Informationssicherheit festzustellen. Noch dieses Jahr wird ein spezieller Cyber-Sicherheits-Check für Industrie 4.0 veröffentlicht. Es stellt sich also nicht die Frage, ob Penetrationstest oder Audit, sondern, in welcher Reihenfolge dies für eine Organisation sinnvoll ist.

Tobias Glemser
tglemser@secuvera.de

Tobias Glemser führt seit dem Jahr 2000 Sicherheitsüberprüfungen sowie Penetrationstests durch und ist Geschäftsführer der secuvera GmbH. Er ist vom Bundesamt für Sicherheit in der Informationstechnik zertifizierter Penetrationstester und Common Criteria Evaluator. Tobias Glemser ist Autor von Fachartikeln und Referent bei Seminaren und Kongressen. Er hat diverse Security Advisories für selbst gefundene Schwachstellen, etwa in Web-Anwendungen, veröffentlicht. Tobias Glemser ist Chapterlead des German Chapter des Open Web Application Security Project (OWASP).