HELPDESK

Security-Tests bringen Licht ins Dunkel

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

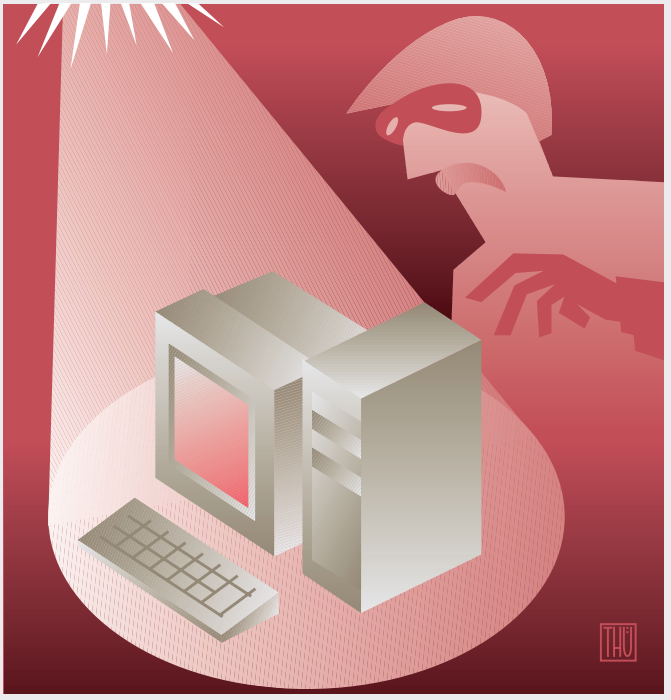

ILLUSTRATION: CW/THÜ

Frage: Wir planen die Durchführung einer technischen Sicherheitsüberprüfung. In den Vorgesprächen mit möglichen Anbietern fiel auf, dass die Anbieter beispielsweise einen Penetration Test unterschiedlich definieren. Gibt es einheitliche Definitionen?

Technische Sicherheitsüberprüfungen bilden eine relativ junge Disziplin, da sie erst mit der wachsenden Popularität des Internets und den damit verbundenen Bedrohungen durch Hacker/Cracker und digitales Ungeziefer allgemein bekannt wurden. Es gibt (noch) keine gängige Definition bezüglich Leistungsumfang, Gemeinsamkeiten und Unterschieden der verschiedenen Testtypen. Die folgenden Informationen sind an die Terminologie des praxisbezogenen «Open Source Security Testing Methodology Manual» (OSSTMM) vom «Institute for Security and Open Methodologies» (ISECOM) angelehnt.

Die Testtypen lassen sich nach der Art des Untersuchungsobjekts, des Vorgehens, der Testtiefe, des Automatisierungsgrads, einer allfälligen Verifikation der Sicherheitslücken und der Manipulation/Modifikation des Untersuchungsobjekts unterscheiden. Bei technischen Sicherheitsüberprüfungen werden primär via Netzwerk ansprechbare Systeme untersucht. «Vulnerability Scans» und «Security Scans» weisen einen sehr hohen Automatisierungsgrad auf, wobei beim Vulnerability Scan keine manuelle Verifikation der von den Scannern detektierten Sicherheitslücken erfolgt. Da Security Scanner nur die bekanntesten Sicherheitslücken erkennen, oft Falschmeldungen generieren und den Kontext des Untersuchungsobjekts nicht berücksichtigen, sind Vulnerability Scans nicht so aussagekräftig wie Security Scans.

> «Es gibt (noch) keine allgemeingültige Definition bezüglich Leistungsumfang, Gemeinsamkeiten und Unterschieden der verschiedenen Testtypen.»

Bei «Penetration Tests» und dem «Ethical Hacking» (auch als Auftragshacking bezeichnet) ist der Anteil an Brainwork wesentlich höher. Automatismen werden nur genutzt, um den Projektfortschritt zu fördern, ohne die Qualität negativ zu beeinträchtigen. Sicherheitslücken werden verifiziert und teilweise auch ausgenutzt. Zwischen den beiden Testtypen bestehen zwei Hauptunterschiede: Einerseits wird das Untersuchungsobjekt nur beim Ethical Hacking beispielsweise mittels Konfigurationsänderungen des Zielsystems oder Einspielen eines Trojaners modifiziert. Dieser kleine Unterschied kann besonders bei streng regulierten Branchen wie der Finanz- und Pharmaindustrie von Relevanz sein. Andererseits sind die Rahmenbedingungen seitens Auftraggeber beim Ethical Hacking weniger eng definiert. So kommen Techniken wie «Dumpster Diving» (Abfall durchsuchen) und/oder «Social Engineering» (Ausnutzen menschlicher Schwächen) oftmals in der Informationsbeschaffungsphase vor dem eigentlichen technischen Hackerangriff zum Einsatz.

Empfehlungen: Anhand des offerierten Aufwands lässt sich abschätzen, ob es sich bei der angebotenen Dienstleistung um einen Test des Qualitätsniveaus «Penetration Test» oder um einen «Security Scan» handelt. Bei Penetration Tests ist mit einem reinen Testaufwand von zirka einem halben Tag pro zu testendes System zu rechnen. Im Gegensatz dazu können bei einem Security Scan 10 bis 200 Systeme pro Tag getestet und ein Teil der Sicherheitslücken manuell überprüft werden. Beim «White Box Approach» wird im Gegensatz zum «Black Box Approach» die Zusammensetzung des Untersuchungsobjekts gegenüber den Testern offen gelegt. Somit bleibt mehr Nettoprojektzeit für die Suche nach Sicherheitslücken übrig. Wer in der Angebotsphase auf einem Ansichtsexemplar eines Schlussberichts und Referenzen (inkl. Ansprechpartner) besteht, kann das Risiko senken, einer Mogelpackung zu erliegen. ■

Der Autor
Christoph Baumgartner ist Consultant und OPST bei der Sicherheitsberaterin Oneconsult, Thalwil, www.oneconsult.com.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch