

Brückenschlag

Quantifizierung operativer Sicherheit

Einführung

Die belegbare Sicherstellung der *IT Security* ist heutzutage von zentraler Bedeutung. Um die Sicherheit von IT Systemen zu beurteilen, stehen grundsätzlich zwei Klassen von Verfahren zur Verfügung: Formale Methoden und Sicherheitstests.

Formale Methoden erlauben es, die Sicherheitsziele eines Systems (wie etwa „Vertraulichkeit“) präzise zu beschreiben und dann zu beweisen, dass keine Attacken existieren, welche diese Sicherheitsziele verletzen. Sowohl die Beschreibung der Ziele als auch der Beweis ihrer Sicherheit geschieht mit mathematischen Mitteln. Verschiedene Bereiche der *IT Security* sind solchen formalen Methoden zugänglich. Ein Paradebeispiel ist die Kryptographie, in welcher etwa die Sicherheit von Verschlüsselungssystemen oder digitalen Signaturen formal bewiesen werden kann. Dennoch erschöpft sich die Anwendbarkeit formaler Methoden auch heute noch auf verhältnismässig wenige Systeme. Die Ausweitung des formalen Ansatzes auf grössere und oft praktisch relevantere Systeme ist Gegenstand der aktuellen *Security*-Forschung.

Die Klasse der Sicherheitstests wiederum ist

reichhaltig und umfasst ad-hoc durchgeführte *Penetration Tests* bis hin zu systematischen Audits und Zertifizierungen. Entsprechend variiert die Aussagekraft der Testergebnisse. Allen Tests ist jedoch gemeinsam, dass nur die Wirkungslosigkeit von bekannten Attacken verifiziert werden kann, nie jedoch ein zuverlässiger Schutz des Systems vor derzeit noch unbekanntem Attacken. Somit liefern Tests schwächere Sicherheitsgarantien als formale Methoden – dafür sind aber komplexe und praktisch relevante Systeme einer Sicherheitsbeurteilung zugänglich.

Standards für IT Sicherheit

Die Sicherung der *IT Security* in Unternehmen und Institutionen – das Security Management – ist ein umfassendes Problem und beinhaltet nebst der technischen IT Komponente auch Fragen von Organisation, Prozess- und Personalmanagement. Auch in Unternehmen spielt die Quantifizierung von Sicherheit eine wichtige Rolle, denn nur dadurch lassen sich Effektivität und Effizienz der implementierten *IT Security* fachgerecht bestimmen. Wichtig ist dabei insbesondere der Fokus auf die operative Sicherheit – also die Sicherheit der IT Systeme selbst und

deren Betrieb – denn damit wird der Schutz der Systeme und Prozesse in der unternehmerischen Praxis gewährleistet.

Der übliche Weg, um dieses Problem anzugehen, besteht in der Implementierung von Standards und Regelwerken, welche von jeder Unternehmung individuell zusammengestellt werden müssen. Bekannte Beispiele sind die BS / ISO Standards (BS 7799, ISO 17799, ISO 27001), ITIL und das BSI Grundschutzhandbuch. Gewiss vermögen diese Standards die generelle Sensibilität für die Probleme des *Security Management* zu erhöhen und manche – so etwa BSI – fokussieren auch direkt die operative Sicherheit. Auch nutzen all diese Standards eine risikobasierte Quantifizierung der operativen Sicherheit. Allerdings geben sie weder Metriken noch Methoden zur Bestimmung der operativen Sicherheit vor.

Resultat dieses Mangels ist, dass Firmen welche Standards implementieren, die operative Sicherheit oft lediglich ad-hoc und somit nicht präzise bemessen. Dadurch entkoppeln sich die implementierten Sicherheitsmanagement-Prozesse von der tatsächlichen operativen Sicherheit – welche letztlich ja das Ziel ist. Mit

anderen Worten: in der Praxis finden sich Unternehmen, die zwar BS / ISO zertifiziert sind, aber deren operative Sicherheit dennoch nicht gewährleistet ist. Ursache dieses Problems ist die fehlende Quantifizierung der operativen Sicherheit.

OSSTMM – Eine Methodologie zur Bestimmung der operativen Sicherheit

Eine Lösung für das oben geschilderte Problem liefert das *Open Source Security Testing Methodology Manual* (OSSTMM) – ein Gerüst zur Integration und Quantifikation von IT Security (siehe <http://www.osstmm.org/>). Diese Methodologie wird von der ISECOM, einer internationalen non-profit Organisation von Security Spezialisten, herausgegeben und stetig weiterentwickelt.

OSSTMM beinhaltet eine Sicherheitsmetrik sowie eine präzise Methodologie zur Bestimmung der operativen Sicherheit gemäss dieser Metrik und ergänzt damit die oben bestehenden Standards. Das Manual beschreibt nebst einer Methodik zur Quantifizierung der Sicherheit, die rechtliche und ethische (Verhaltenskodex) Basis für die Durchführung von Sicherheitsaudits.

Der erste Schritt eines Audits nach OSSTMM ist die Festlegung des *Scope* des Audits: Hierbei wird definiert welche strategischen Vorgaben gelten und operativ abgebildet werden müssen, sowie was für Objekte und in welcher Tiefe untersucht werden sollen. Nur dadurch lässt sich Sicherheit über Jahre hinweg vergleichbar und somit nachhaltig messen und gewährleis-

ten. Zu diesem Zweck müssen insbesondere müssen so genannte „Changes“ minutiös genau verfolgt werden.

Nach der Definition des *Scope* wird die operative Sicherheit anhand der im Manual beschriebenen Werkzeuge – umfassende Kataloge von Tests und Test-Szenarien – bemessen. Das OSSTMM bietet auch Hilfestellung für die Interpretation der vorgenommenen Analyse und der dadurch erzielten Resultate. Es gibt schliesslich ein *best practice* Modell vor – also konkrete Vorgaben für Programmierung, Netzwerk- und Serverkonfiguration, sowie Hinweise für das Erstellen einer *gap*-Analyse und eines Behebungsplans.

Dadurch entsteht eine rein operative Metrik, welche Sicherheit messbar und damit plan- und budgetierbar macht. Diese Metrik dient dann auch als Schnittstelle zu rein strategischen Verfahren, die in den erwähnten generellen Standards beschrieben sind. Betriebliche Aspekte lassen sich damit optimal in die strategische Führung integrieren.

OSSTMM kann schliesslich auch für die Zertifizierung von Produkten mit sicherheitsrelevanten Features verwendet werden. Der Käufer dieses Produkts erhält damit die Gewissheit, dass das Produkt den massgeblichen Sicherheitsvorgaben auch in quantitativer Hinsicht genügt.

Die Tester ausbilden

Eine zentrale Komponente für die Qualität und Aus-

sagekraft von Sicherheitstests ist natürlich der Tester selbst. Dieser grundlegende Aspekt bedingt denn auch eine Ausbildung der Tester, welche das OSSTMM verwenden wollen, um dadurch den durch das Manual vermittelte Qualitätslevel auch erreichen zu können. Insofern bilden Kurse und eine damit verbundene Zertifizierung der Tester Bestandteil des OSSTMM.

Dazu existieren drei Kurse für Tester, für Analysten, sowie für Projektleiter von Sicherheitsprojekten („Opst OSSTMM Professional Security Tester“, „Opsa OSSTMM Professional Security Analyst“, „Opse OSSTMM Professional Security Expert“). An der Berner Fachhochschule werden diese Kurse den Studierenden als Wahlfach angeboten. Sie erhalten dadurch nicht nur wichtiges Wissen für ihre Bewährung auf dem *Security* Arbeitsmarkt, sondern gewinnen gleichzeitig auch tiefere Einblicke in das Wesen von Sicherheit und ihrer Validierung.

Hierbei ist klar, dass Zertifizierungen lediglich eine solide und hinreichende Qualifikation des Testers sicherstellen können, aber nicht in der Lage sind Unterschiede im Know-How und Erfahrung auszunivellieren. Die Abhängigkeit der Qualität von Security Tests vom Tester wird sich nie gänzlich aufheben lassen. Die Erfahrung zeigt aber, dass von Testern gleicher Qualifikationsstufe unabhängig durchgeführte OSSTMM Audits zu (von minimalen Abweichungen abgesehen) denselben Resultaten führen. Mehr kann man von einem Sicherheits-

test wahrlich nicht erwartet
werden.

Autoren

Dr. Endre Bangerter, Berner
Fachhochschule - Technik
und Informatik, Professor für
IT Security.

Nicolas Mayencourt, Gründer
und CEO der Dreamlab AG
und Mitglied im Verwaltungsrat
der ISECOM.