Dirk Fox

Penetrationstest

Hintergrund

Unter einem Penetrationstest wird ein systematischer Eindringversuch in ein IT-System oder eine IT-Infrastruktur bezeichnet, der mit Einverständnis oder im Auftrag des Betreibers durchgeführt wird. Er soll dazu dienen, die Resistenz der untersuchten Systeme gegen einen „Angriff" auf die Infrastruktur unter Verwendung informationstechnischer Mittel zu prüfen.

Üblicherweise werden bei einem Penetrationstest Tools eingesetzt, die auch Angreifern zur Verfügung stehen, um nicht durch Software-Updates beseitigte, bekannte Schwachstellen der eingesetzten Soft- und Hardware zu identifizieren und von außen erreichbare Dienste und Systeme zu erkennen.

Meist endet ein Penetrationstest kurz vor dem Eindringen in das untersuchte IT-System oder die –Infrastruktur; es wird lediglich aufgezeigt, welche Möglichkeiten einem Angreifer durch die Ausnutzung einer gefundenen Schwachstelle zur Verfügung stehen würden.

Zwar steht bei einem Penetrationstest in der Regel die Internet-Schnittstelle im Zentrum der Untersuchung. Da es aber häufig weitere kommunikationstechnische Zugänge zum Unternehmen (wie z. B. die Telefonanlage) gibt, werden diese sinnvoller Weise in einen Penetrationstest einbezogen.

Durchführung

Penetrationstests simulieren einen Angriff auf ein IT-System oder eine IT-Infrastruktur. Anders als ein echter Angreifer nutzen sie die gefundenen Schwachstellen nicht aus, sondern protokollieren alle sicherheitsrelevanten „Findings". Sie stoppen auch nicht, wenn sie eine wirkungsvoll nutzbare Schwachstelle gefunden haben, sondern prüfen die Anfälligkeit des Zielsystems für jede bekannte Angriffsmethode.

Bei der Konzeption des Penetrationstests sollten auch unterschiedliche Angreiferperspektiven eingenommen werden, wie ein Angriff von außen auf die DMZ (die durch Firewalls geschützten, von außen erreichbaren Server), ein Angriff aus der DMZ (Simulation eines übernommenen DMZ-Rechners) und ein Angriff aus dem internen Netz [1, 2, 3].

Auch wenn Penetrationstester nicht in Systeme eindringen, können sie mit den durchgeführten Tests Systeme (unbeabsichtigt) destabilisieren oder sogar zum Absturz bringen. Daher müssen Penetrationstests eng zwischen Tester und Auftraggeber abgestimmt werden, damit produktive Systeme nur zu ausgewählten Zeiten untersucht und im Falle eines Ausfalls zügig wieder in Betrieb genommen werden können.

Werden Schwachstellen von erheblicher Bedeutung gefunden, wird der Auftraggeber in der Regel unverzüglich unterrichtet, damit die Schwachstelle umgehend beseitigt werden kann.

Penetrationstests sollten grundsätzlich von externen Fachkräften, mindestens aber von einer von der IT unabhängigen Einheit (IT-Revision) durchgeführt werden, um das Übersehen von Schwachstellen durch „Betriebsblindheit" zu vermeiden.

Aussagekraft

Ein Penetrationstest ist naturgemäß immer eine „Momentaufnahme": Jede anschließende Änderung der Konfiguration kann zu einer abweichenden Bewertung führen. Dennoch gibt die Zahl und das Alter der gefundenen schwer wiegenden Schwachstellen einen Hinweis auf das Sicherheitsniveau des Systems.

Auch liefert ein Penetrationstest – abgesehen von generellen Empfehlungen wie der Deaktivierung nicht benötigter Dienste – immer nur Feststellungen von bereits bekannten Schwachstellen, da Tools und Tester auf dieser Wissensbasis aufsetzen. Durch das Bekanntwerden neuer Angriffsmöglichkeiten kann das Ergebnis schon kurze Zeit nach Durchführung des Tests ganz anders ausfallen. Existieren „Zero-Day-Exploits", die eine bisher nicht allgemein bekannte Schwachstelle nutzen, kann auch bei einem Testergebnis ohne wesentliche Auffälligkeiten die Infrastruktur elementar bedroht sein.

Penetrationstests liefern auch keine Aussagen über das Sicherheitsmanagement – also den strukturierten und systematischen Umgang mit dem Thema Informationssicherheit im untersuchten Unternehmen: So kann eine Infrastruktur technisch solide abgesichert sein – aber das Wissen über die Gesamtkonfiguration allein im Kopf eines Administrators stecken.

Trotz dieser Einschränkungen sind regelmäßige Penetrationstests ein wichtiges Element des Sicherheitsmanagements. Sie zwingen Administratoren und Betreiber, sich der Weiterentwicklung von Angriffstechniken und der Änderung der Bedrohungslage zu stellen und für eine ständige Anpassung der Konfigurationen und Regelwerke zu sorgen.

Kombiniert man Penetrationstests mit Sicherheitsaudits [2], bei denen auch die Dokumentation, Struktur und Ausgestaltung des Sicherheitsmanagements untersucht werden, gewinnt man ein aussagekräftiges Gesamtbild des im Unternehmen erreichten Sicherheitsniveaus.

Referenzen

[1] Gora, Stefan: Security Audits. Datenschutz und Datensicherheit (DuD), Gateway, 2/2007, S. 120.
[2] Gora, Stefan: Security Audits. Datenschutz und Datensicherheit (DuD), 4/2009, S. 238-246.
[3] Schreiber, Sebastian: Penetrationstests planen. Datenschutz und Datensicherheit (DuD), in diesem Heft.