IT-Sicherheit

# Penetrationstests decken IT-Sicherheitslücken rechtzeitig auf

**Von Christian Scharff**

*Schwachstellen in der Unternehmens-IT selbst erkennen, bevor sie ein Angreifer finden und ausnutzen kann – das ist die Idee eines Penetrationstests. Sorgfältig geplant und von einem professionellen Dienstleister auf Netzwerk- und Systemebene oder auf Applikationsebene vorgenommen, erweist sich solch ein Test als effiziente Massnahme gegen die wachsende Bedrohung durch Cyberkriminalität.*

Cybersecurity und IT-Sicherheit gehören nach wie vor zu den wichtigsten Digitalthemen 2016. Zu Recht, wie auch eine aktuelle Umfrage des Branchenverbandes Bitkom (www.bitkom.org) zeigt. Über zwei Drittel der befragten Industrieunternehmen gaben darin an, in den letzten zwei Jahren Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden zu sein.

Wie gefährdet aber ist das eigene Unternehmen? Um das realistisch einschätzen und rechtzeitig gegensteuern zu können, empfiehlt sich die Durchführung eines Penetrationstests. Ähnlich einer Brandschutzübung wird dabei der Ernstfall simuliert, in diesem Fall ein Angriff auf die Daten- und IT-Systeme des Unternehmens. Ziel ist es, Schwachstellen in IT-Systemen, Software oder deren Konfiguration präventiv zu erkennen. Im Falle eines tatsächlichen Angriffs könnten diese Sicherheitslücken sonst von Hackern ausgenutzt werden, um Zugriff auf die Systeme zu erhalten, an sensible Informationen zu gelangen oder die Verfügbarkeit von Systemen und Anwendungen einzuschränken.

**Dr.-Ing. Christian Scharff** ist zertifizierter Informationssicherheits-,Revisions- und Beratungsexperte (BSI) sowie zertifizierter Datenschutzauditor (TÜV).
Weitere Informationen: www.accuris.de

## Der Ernstfall wird simuliert

Mit der professionellen, an realistischen Szenarien orientierten Durchführung eines Penetrationstests werden in der Regel externe, auf Sicherheitstests spezialisierte Dienstleister beauftragt. Deren Vorgehen folgt wie das tatsächlicher Angreifer einem bestimmten Muster: Am Anfang steht die Informationsbeschaffung, dazu werden öffentlich zugängliche Informationen über die Zielsysteme ausgewertet, z.B. aus DNS- und WHOIS-Datenbanken und Google-Hacking-Techniken sowie durch Mitschneiden des Netzwerkverkehrs (Sniffing). Über Portscans erfolgt dann die Identifizierung offener TCP- und UDP-Ports. Welche Betriebssystem- und Softwareversionen im Unternehmen verwendet werden, lässt sich mittels Banner-Grabbing und Software-Fingerprints bestimmen. Die so identifizierten Netzwerkdienste und Betriebssystemversionen werden dann zunächst mit automatisierten Schwachstellenscannern auf bekannte Schwachstellen hin überprüft. Die Ergebnisse dieser Scans werden dann durch manuelle Überprüfungen verifiziert – um «False Positives» zu eliminieren, aber auch um mögliche zusätzliche Schwachstellen auszumachen.

**Worauf ist zu achten, wenn man einen externen Dienstleister mit einem Penetrationstest beauftragt?** Zunächst einmal sollten die Testinhalte und -ziele möglichst konkret vorgegeben sein. Solche Vorgaben könnten sein:

- *Ermittlung und Versuch der Ausnutzung von Implementierungsschwächen des Betriebssystems oder fehlerhafter Konfigurationen des Zielsystems – etwa durch Zugriff auf beliebige Dateien auf einem IIS-Server*
- *Untersuchung auf unerwünscht zulässige Dienste, die z.B. durch fehlerhafte Konfiguration oder unzureichende Filterregeln ermöglicht werden*
- *der Versuch, eingesetzte Dienste durch Denial-of-Service-Attacken (DoS) ausser Kraft zu setzen oder DoS-Attacken nur nach expliziter Freigabe durch den Auftraggeber zu starten.*

## Risiken erkennen und minimieren

Der letzte Punkt macht deutlich, dass Penetrationstests immer auch mit Risiken verbunden sind. Denial-of-Service-Angriffe werden in der Praxis nur durchgeführt, wenn der Auftraggeber dies ausdrücklich wünscht. Aber auch ohne solch hochriskante Angriffe kann ein Penetrationstest zum Verlust der Verfügbarkeit von Systemen führen, wenn etwa das betroffene System nach einem Absturz erst durch einen lokalen Administrator manuell neu gestartet werden muss. Eine weitere unbeabsichtigte Folge eines Penetrationstests kann Datenverlust sein.

Abhängig von der Zielumgebung können diese Gefahren ein nicht zu akzeptierendes Risiko darstellen. Für Produktionssysteme gilt das in besonderem Masse. Diese Systeme können dann von riskanten Tests ausgenommen werden. Dies mindert jedoch auch immer die Aussagekraft des Tests, denn reale Angreifer machen nicht halt vor den Produktivsyste-

men. Kritische Schwachstellen könnten übersehen werden. Eine Alternative dazu ist es, den Test ausserhalb der Geschäftszeiten durchzuführen oder in einer identischen Testumgebung, die die Produktivumgebung 1:1 nachbildet. Ein möglicher Schaden für Produktivsysteme im Falle eines Ausfalls lässt sich so vermeiden oder zumindest verringern.

Da ein Restrisiko für die untersuchten Systeme und Daten jedoch nie vollständig ausgeschlossen werden kann, ist es essenziell, Penetrationstests vorab sehr gründlich von der IT-Abteilung des Auftraggebers und dem Penetrationstester gemeinsam zu planen. Während der Durchführung sollte laufend ein technischer Ansprechpartner zur Koordination erreichbar sein.


Quelle: Depositphotos

*Wirtschaftskriminelle suchen jegliche Lücken in IT-Systemen, in der Software oder in der aktuellen Konfiguration.*

## Durchführungsoptionen richtig kombinieren

Penetrationstests können in mehreren Varianten durchgeführt werden, meist werden dabei mögliche Optionen kombiniert.

## Black-Box vs. White-Box

Zunächst lassen sich «Black-Box»- und «White-Box»-Tests unterscheiden. Im Falle des Black-Box-Tests werden dem externen Dienstleister nur die nötigsten Informationen, wie etwa der Name des zu testenden IT-Verbunds zur Verfügung gestellt – um die Möglichkeiten eines externen Angreifers möglichst realistisch nachzustellen. Der Angreifer recherchiert dann den IP-Adressbereich und mögliche «Einfallstore». Auch die Überprüfung der Funktionsweise von IDS/IPS-Systemen sowie des Verhaltens und der Reaktionsgeschwindigkeit der eigenen Mitarbeiter kann ein Teilziel eines Black-Box-Tests darstellen.

Allerdings ist diese Vorgehensweise sehr zeitaufwendig und damit sehr kostenintensiv. Beim tatsächlichen Angreifer ist davon auszugehen, dass sie sich die nötige Zeit für die Planung und Vorbereitung nehmen würden. Deren Angriffe werden zunehmend komplexer und technisch ausgefeilter und meist werden auch Social-Engineering-Methoden zur Informationsbeschaffung genutzt. Nicht immer sind diese Methoden leicht zu erkennen, so werden zum Beispiel die Absenderadressen von E-Mails anderer Firmen gefälscht und genau auf den Empfänger, dessen Interessen und Bekanntenkreis zugeschnittene Pishing-Mails versendet (Spear Pishing), um Schadsoftware zu injizieren. Mithilfe der injizierten Schadsoftware werden alle benötigten Informationen aus dem angegriffenen IT-Verbund alle erforderlichen Informationen beschafft.

Um diesen «Vorteil» potenzieller Hacker gegenüber dem in begrenztem Zeitrahmen agierenden IT-Dienstleister auszugleichen, greift man bei der Durchführung von Penetrationstests auf das White-Box-Verfahren zurück. Dabei werden dem Penetrationstester ausführliche Informationen über die zu testenden Systeme und die Netzwerkinfrastruktur zur Verfügung gestellt. Damit ist der Tester zu Beginn der Penetrationstests auf dem Informationsstand eines realen Angreifers nach wochenlanger Arbeit. So lassen sich auch Schwachstellen finden, die sonst in einem reinen Black-Box-Test möglicherweise nicht erkannt würden. In der Praxis kommt meist ein Mix aus Black-Box- und White-Box-Pen-Test zum Einsatz.

## On-Site vs. Off-Site

Die zweite Unterscheidung betrifft den Punkt, von dem aus getestet/angegriffen wird. Penetrationstests können off-site über das Internet oder aber im Inneren des Unternehmensnetzes selbst, also on-site, durchgeführt werden.

Off-Site-Penetrationstests haben den Vorteil, dass sie sehr kostengünstig sind und dem Angriffsvektor eines potenziellen Angreifers aus dem Internet entsprechen. Ihre Aussage ist jedoch eingeschränkt: Ein verwundbarer Dienst etwa, der während des Tests von einer vorgelagerten Firewall geblockt wurde, würde nicht identifiziert werden.

Mit einem On-Site-Test aus der demilitarisierten Zone (DMZ) heraus lässt sich dagegen simulieren, dass ein Angreifer ein System, z. B. einen Webserver, bereits übernommen hat. Im Falle einer solchen mehrstufig aufgebauten Sicherheit, mit einer Firewall zwischen Internet und DMZ sowie zwischen DMZ und Office, lässt sich die Sicherheit wesentlich umfassender prüfen. Eine hiernach verifizierte Defense-In-Depth-Sicherheit bietet auch bei der Kompromittierung eines Systems aus der Sicherheitskette noch ausreichenden Schutz zur Abwehr eines Angreifers. Zudem lassen sich über On-Site-Tests auch die Bedrohungen durch Innentäter oder Insider prüfen – ein nicht zu unterschätzendes Risiko: Laut der eingangs erwähnten Bitkom-Umfrage standen in 65 Prozent der Fälle aktuelle oder ehemalige Beschäftigte hinter den Angriffen.

Den wirkungsvollsten und umfassendsten Ansatz bietet letztlich die Kombination der verschiedenen Optionen: Black-/White-Box, Off-Site-/On-Site-Tests, um alle Bedrohungsszenarien abzudecken, sowie die Ergänzung automatischer Scanner durch manuelle Methoden. Ein sorgfältig geplanter Penetrationstest ist somit eine wirksame Massnahme zur Absicherung gegen potenzielle Bedrohungen und für diesen Zweck auch effizienter und kostengünstiger als ein vollständiges Systemaudit – vorausgesetzt natürlich, die identifizierten Schwachstellen werden anschliessend behoben. ■