Bedrohungen frühzeitig erkennen

Die globale Vernetzung hat die Computerwelt revolutioniert, aber im gleichen Mass wie die technischen Möglichkeiten sind auch die entsprechenden Bedrohungen stetig angewachsen. Die Computersicherheit ist für viele Firmen zum überlebensnotwendigen Faktor geworden – Forschungsergebnisse oder eigene Produktentwicklungen, die auf firmeninternen Servern liegen, locken virtuelle Langfinger aus aller Welt an. Zur Abwehr von Angriffen muss man verstehen, wie ein Angreifer vorgeht.

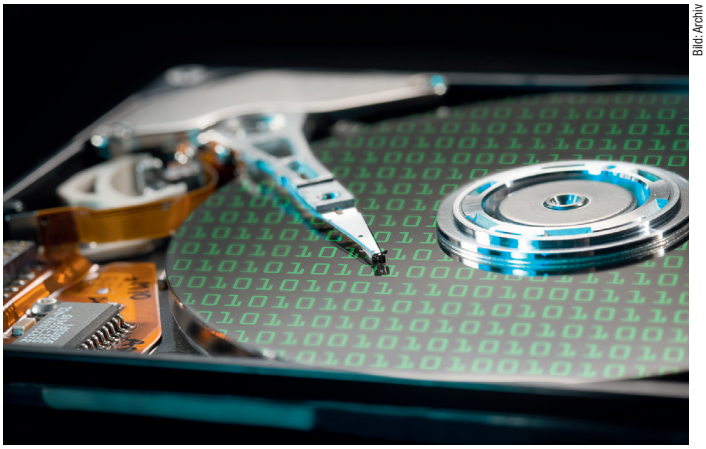

Bild: Archiv

Verstehen wie ein Angreifer vorgeht.

Ein professioneller Penetrationstest ist elementarer Teil jedes Sicherheitsaudits und überprüft Ihr Netzwerk systematisch auf Schwachstellen und Sicherheitslücken. Damit wendet der IT-Penetrationstest eine Vorgehensweise an, die im Wesentlichen der eines Hackerangriffs entspricht. Penetrationstests (Eindringversuche in Computernetze) lassen sich in sieben Phasen gliedern.

Phase 1

In der ersten Phase werden Ihre Erwartungen geklärt und Ihre Ziele festgelegt. Es werden Eskalationsstufen für den Notfall fixiert und Ansprechpartner genannt. Die Sicherheitsanalyse wird näher klassifiziert und ein Testzeitraum wird bestimmt.

Phase 2

In der zweiten Stufe wird über das Zielsystem recherchiert. Es werden hierbei Informationen herangezogen, die im Internet verfügbar sind. Dazu zwei Beispiele: Jedes im Internet erreichbare Rechnersystem muss über eine offizielle IP-Adresse verfügen. Frei zugängliche Datenbanken liefern Informationen über IP-Adressblöcke, die einer Organisation zugewiesen sind. (Dies gilt natürlich nur für statische IP-Adressen.) Weiterhin ist es möglich, dass Einzelheiten über das vom Kunden eingesetzte System und seine Konfiguration zum Beispiel in News-Gruppen oder Web-Foren zu finden sind.

Phase 3

Nun wird Ihr Computersystem zum ersten Mal aktiv einer Prüfung unterzogen. Es werden das Betriebssystem des Rechners und die angebotenen Dienste eruiert.

Hierbei wird auch versucht, den oder die zu überprüfenden Rechnersysteme unter anderem einem sogenannten Portscan zu unterziehen. Offene Ports lassen Rückschlüsse auf die zugeordnete Anwendung zu.

Über das sogenannte «Fingerprinting» können Namen und Version von Betriebssystemen und Anwendungen auf dem Zielsystem in Erfahrung gebracht werden. Teilweise erfolgt auch der Einsatz von automatisierten Schwachstellenscannern. Sinnvoll eingesetzt, beschleunigen sie die Prüfung. Diese Scanner stossen jedoch bei ungewöhnlichen Kombinationen an ihre Grenzen und können konstruktionsbedingt nicht alle Schwachstellen erkennen. Daher können sie das manuelle Vorgehen nicht ersetzen.

Als Abschluss erfolgt eine erste Bewertung der Zielsysteme, wobei grobe Aufwandsabschätzungen für einen potenziellen Einbrecher erfolgen.

Phase 4

In der vierten Stufe der Sicherheitsanalyse erfolgt die Schwachstellenrecherche. Mit den gewonnenen Informationen wird die zielgerichtete Suche über Schwachstellen bestimmter Betriebssysteme und Anwendungen durchgeführt. Ist ein Exploit (Programm zur Ausnutzung der Schwachstelle) verfügbar, wird es Bestandteil des Angriffs werden.

Phase 5

Hier werden die gefundenen Schwachstellen ausgenutzt. Der Zweck ist, Zugriff zum System zu erhalten beziehungsweise weitere Angriffe vorzubereiten. Es werden gezielte Attacken gegen die Rechnersysteme ausgeführt.

Phase 6

Im sechsten Stadium der Sicherheitsanalyse erfolgt die Abschlussbewertung. Der Abschlussbericht wird erstellt und eine Managementzusammenfassung wird angefertigt. Die Zusammenfassung beinhaltet den Prüfungsauftrag, die wesentlichen Prüfungsergebnisse und weitere empfohlene Vorgangsweisen in leicht verständlicher Sprache. Logfiles, Einsatzzeiten (welcher Angriff wurde zu welcher Zeit ausgeführt) und weitere Arbeitsergebnisse werden beigelegt.

Phase 7

Abschliessend wird ein Nachtest absolviert. Vor allem wenn in vorangegangenen Phasen Mängel gefunden wurden, hat sich dies als sehr sinnvoll erwiesen. Ziel dieses Tests ist es, die Wirksamkeit von Sicherungsmassnahmen zu überprüfen. Der Nachtest erfolgt in der Regel etwa 30 Tage nach dem Penetrationstest.

INFOS | KONTAKT

iMes Solutions GmbH
Elisabethstrasse 8
D-84489 Burghausen

Telefon +49 (0)8677 9618-0
www.imes-solutions.com
info@imes-solutions.com