Security

eXtreme Hacking!

Häufig ist Unternehmen nicht bewusst, welchen Gefahren sie durch Hacking-Attacken ausgesetzt sind.

Die fünftägige Schulung „eXtreme Hacking" der Wirtschaftsprüfungsgesellschaft Ernst & Young AG vermittelte die Methoden sowie Vorgehensweisen von „Hackern" und versetzte die Teilnehmer in die Lage, die Risiken eigener IT-Systeme und Infrastrukturen zu erkennen und diese entsprechend abzusichern.

Bereits zum zweiten Mal in einem Jahr fand Ende 2003 die deutsche Veranstaltung in Eschborn/Frankfurt am Main statt und veranschaulichte sehr praxisnah die Methoden und Vorgehensweisen von Hackern. Die Schulung, die von Ernst & Young vor Jahren in den USA konzipiert wurde und seitdem weltweit für alle Mitarbeiter im Bereich IT-Security verpflichtend ist, wird aufgrund der hohen Nachfrage am Markt seit 1999 auch für Kunden angeboten. Die Basis dieser Schulung ist eine spezielle, von Ernst & Young entwickelte und in dem Buch „Hacking Exposed" publizierte Vorgehensweise.

Am ersten Tag, der unter dem Motto Discovery/Scanning stand, zeigten die IT-Sicherheitsexperten von Ernst & Young nach einer allgemeinen Einführung verschiedenste Techniken (z. B. Banner Retrieval, Portscans, DNS-Zonentransfer), um Zielsysteme sowie die auf dem Zielsystem installierten Applikationen und das zugrunde liegende Betriebssystem eindeutig zu identifizieren. Wie jeden Tag endete auch dieser mit einer langen Open End-Session, in der die Teilnehmer das in der Schulung erlangte Wissen an verschiedensten Testsystemen direkt in die Tat umsetzen konnten.

Der darauf folgende Tag beschäftigte sich ausschließlich mit Windows NT, 2000 und XP-spezifischen Angriffen und veranschaulichte durch die sehr strukturierte Vorgehensweise der IT-Experten von Ernst & Young, welche potenziellen Sicherheitslücken auf diesen Betriebssystemen existieren und wie diese durch Hacker ausgenutzt werden können, um privilegierten Systemzugriff zu erhalten. Dabei wurde durch die Referenten Krisztian Piller und Marcus Rubenschuh dargestellt, dass neben einer ganzen Reihe von neuen Techniken ein Großteil der Windows NT-spezifischen Angriffe auch gegen die heutzutage weit verbreiteten Varianten 2000 und XP möglich sind. Ein finales Übungsszenario, in dem die Teilnehmer anhand verschiedenster Aufgaben (Enumeration der Domäne, Identifizierung der Systeme innerhalb der Domäne, Ermittlung der Benutzerinformationen der Zieldomäne etc.) das Gelernte in die Praxis umsetzen konnten, vervollständigte den zweiten Tag.

Der dritte Tag, der unter dem Motto Unix stand, widmete sich primär der Sicherheit von Unix- und Linux-basierten Systemen und zeigte die vielseitigen Angriffsmöglichkeiten auf derartige Betriebssysteme. Nach einer Identifikation des entfernten Betriebssystems mit passiven und aktiven Techniken erfolgte eine detaillierte Analyse sowie eine Ermittlung der potenziellen Schwachstellen der festgestellten Systeme.

Dabei stellten die Referenten zahlreiche lokal und entfernt durchführbare Angriffsvarianten auf die bekannten Netzwerkdienste (z. B. NFS, FTP, DNS, HTTP, X-Window etc.) vor und veranschaulichten diese durch praktische Beispiele. Schließlich stellten sie Methoden zur lokalen und entfernten Rechte-Eskalation (z. B. Buffer Overflows, Race Conditions) vor und zeigten entsprechende Gegenmaßnahmen auf, die erfolgreiche Angriffe auf Unix- bzw. Linux-Systeme verhindern sollen.

Zu guter Letzt konnten die Teilnehmer die neuen Techniken an speziell präparierten Testsystemen ausprobieren und versuchen, die gestellten Aufgaben (Angriff mehrerer Systeme durch verschiedenste Protokolle, Erlangung von privilegiertem Benutzerzugriff) erfolgreich zu absolvieren.

Das Motto des nächsten Tages lautete Web Applications/Firewalls und beschäftigte sich mit der Sicherheit von Web Applikationen und Firewalls. Die Experten von Ernst & Young stellten zunächst verschiedenste Methoden vor, um die Arten und Versionen von Webservern sowie die auf diesen verfügbaren Technologien und Anwendungen zu identifizieren. Daraufhin veranschaulichten sie zahlreiche, teilweise anwendungsspezifische Techniken (z. B. Buffer Overflows, Directory Traversal, Umgehung von Intrusion Detection Systemen, Brute Force-Angriffe, SQL Injection), die von Hackern angewendet werden, um Webserver (z. B. Apache, Netscape Enterprise Server, Lotus Domino oder Microsoft Internet Information Server) oder darauf laufende Anwendungen gezielt anzugreifen und für ihre Zwecke zu missbrauchen.

Schließlich gaben sie wertvolle Hinweise und zeigten geeignete Gegenmaßnahmen auf, um derartige Angriffe zu unterbinden. Des weiteren veranschaulichten die Referenten an diesem Tag die Identifikation von Firewalls sowie die Analyse der verschiedenen Arten von Firewalls. Außerdem zeigten Sie die möglichen Angriffsformen gegen Firewalls und stellten mehrere Möglichkeiten vor, diese zu umgehen (z. B. ICMP- oder HTTP-Tunneling). Wie immer wurde auch dieser Tag durch eine lange Open End-Session, in der die Teilnehmer verschiedenste Aufgaben bewältigen mussten, beendet.

Der letzte Tag widmete sich den Themengebieten Mainframes, Databases sowie Advanced Techniques und gab den Teilnehmern, neben einem Überblick über die verschiedenen Angriffsmöglichkeiten gegen Mainframes und Datenbanksysteme (z. B. Oracle, MS-SQL, Sybase), einen gründlichen Einblick in die fortgeschrittenen Techniken (z. B. Spoofing, Hijacking, Port-Redirection, Backdoors, Rootkits, DNS Poisoning, Social Engineering etc.), die von Hackern angewendet werden, um in Systeme aller Art einzudringen. Die finalen Übungen des Tages, in denen die Teilnehmer einen Großteil der gelernten Methoden der vergangenen Tage nochmals ausprobieren konnten, rundeten die Veranstaltung ab.

Weitere Informationen zu denen von Ernst & Young angebotenen Dienstleistungen im Bereich IT-Security erhalten Sie unter www.de.ey.com/hacking.

Sebastian Wolfgarten