

Penetrationstest: Wie «wasserdicht» ist die Sicherheit Ihrer Systeme?

Wolfgang Sidler

Systeme, die über Verbindungen zu öffentlichen Netzen verfügen, unterliegen in besonderer Weise unautorierten, meist anonymen Zugriffsversuchen. In dieser Situation werden Testmethoden benötigt, die sich des Blickwinkels der Angreifer bedienen, um möglichst reale Testbedingungen zu schaffen.

Im technischen Sprachgebrauch versteht man unter einem Penetrationstest den kontrollierten Versuch, von «ausen» in ein bestimmtes Computersystem bzw. -netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden die gleichen Techniken wie auch bei einem realen Angriff eingesetzt. Die so identifizierten Schwachstellen lassen sich durch entsprechende Massnahmen beheben, bevor diese von unautorisierten Dritten genutzt werden.

Täterprofile

Üblicherweise wird in der medialen Berichterstattung unter dem Begriff «Hacker» pauschal jemand bezeichnet, der unbefugt in fremde IT-Systeme eindringt. Oftmals wird jedoch zwischen «Hackern», «Crackern» und «Script Kiddies» unterschieden. Während «Hacker» dabei als experimentierfreudige Programmierer angesehen werden, die sich aus technischem Interesse mit Sicherheitslücken in IT-Systemen auseinandersetzen, werden unter «Crackern» Personen verstanden, die sich aufgrund krimineller Energie der Schwachstellen von IT-Systemen bedienen, um dadurch rechtswidrige Vorteile oder gesellschaftliche Aufmerksamkeit bzw. Anerkennung zu erlangen.

Mit der Verbindung zum Internet als öffentliches und damit unsicheres Netzwerk sind verschiedene Risiken verbunden. Durch den zweckmässigen Einsatz diverser technischer Mittel und das Einhalten von Richtlinien können diese Risiken auf ein vertretbares Mass reduziert werden.

Bei «Script Kiddies» handelt es sich meist um Täter, die ohne umfangreiches Hintergrundwissen und aus Neugier weitestgehend vorgefertigte Angriffstools aus dem Internet gegen willkürlich ausgewählte oder besonders exponierte Ziele anwenden. Cracker, die über privilegiertes Wissen über die Organisation, die sie angreifen wollen verfügen, werden als Insider bezeichnet, oft frustrierte (ehemalige) Mitarbeiter einer Organisation, die ihr Wissen dazu nutzen, der Organisation Schaden zuzufügen. Gefahr die von Insidern ausgeht, ist als besonders hoch einzuschätzen, da sie mit der technischen und organisatorischen Infrastruktur vertraut sind und vorhandene Schwachstellen möglicherweise bereits kennen. Neben den oben beschriebenen Tätergruppen stellt auch die Wirtschaftsspionage eine ernst zu nehmende Bedrohung dar: Ihr Ziel ist es, von Betriebsgeheimnissen wie innovativen technischen Konzepten, Strategien und Ideen, die einen Wettbewerbsvorteil bedeuten, Kenntnis zu erlangen um sie zum eigenen Vorteil zu nutzen.

Vorgehensweise der Täter

Es existieren mehrere Möglichkeiten, IT-Systeme zu manipulieren oder zu schädigen bzw. einen Angriff vorzubereiten. Unter «Angriffe über das Netzwerk» versteht man Attacken, die unter Nutzung von Funktionalitäten der eingesetzten Netzwerkprotokolle auf Netzwerkkomponenten, Computersysteme und oder Applikationen stattfinden. Diese Art von Angriffen nutzt Schwachstellen oder Unzulänglichkeiten in Hard- und Software,



um Angriffe vorzubereiten oder durchzuführen. Angriffe über das Netzwerk sind Portscanning, IP-Spoofing, Sniffing, Session Hijacking, DoS-Attacken, Buffer-Overflow- bzw. Format-String-Attacken sowie jegliches weitere Ausnutzen von Schwachstellen in Betriebs- und Anwendungssystemen und Netzwerkprotokollen.

Bei sog. Social Engineering-Angriffen wird versucht, Menschen mit privilegier-

tem Wissen soweit zu manipulieren, dass sie dem Angreifer sicherheitsrelevante Informationen, wie z.B. Passwörter, preisgeben. So kann sich ein Angreifer als IT-Mitarbeiter einer Organisation ausgeben und dadurch einen arglosen Benutzer unter einem Vorwand dazu bringen sein Netzwerkpasswort herauszugeben. Besonders hier ist die Variationsmöglichkeit von Angriffsszenarios sehr hoch. Im weitesten Sinne könnte man auch Szenarien, in denen Erpressung als Mittel zur Herausgabe von sicherheitsrelevanten Informationen eingesetzt wird, als Social Engineering bezeichnen. Die physische Sicherheit der technischen Infrastruktur ist eine Grundvorausset-



zung zur Gewährleistung von IT-Sicherheit. Wenn physische Sicherheitsmassnahmen überwunden werden können und auf diese Weise Zugriff erlangt wird, ist es meist nur eine Frage der Zeit, bis auch ein Zugriff auf bzw. die Manipulation der gespeicherten Anwendungen und Daten stattfinden kann. Das unbefugte Eindringen in das Rechenzentrum einer Organisation und das Entwenden einer Festplatte mit vertraulichen Daten oder

das Durchsuchen von Abfällen nach Dokumenten mit sicherheitssensitiven Informationen (Dumpster Diving) gehören zu dieser Gruppe.

Der Penetrationstest

1995 wurde der Begriff «Penetrationstest» und die dafür durchgeführten Methoden durch die Veröffentlichung des ersten Unix-basierten Schwachstellen-Scanner «SATAN» (Venema95) etabliert. Es war das erste Tool das automatisiert Rechner auf Schwachstellen untersuchen konnte. Unter dem Begriff Penetrationstest versteht man den Versuch, autorisiert in ein Netzwerk einzubrechen, um Aufschluss über dessen Sicherheitsniveau zu erhalten. Ziele können zum Beispiel eine Firewall, ein Mail-, Web- oder Datenbankserver, Applikationen oder das ganze Netz sein. Wichtig ist jedoch, dass ein Penetrationstest nur teilweise vorhandene Schwachstellen aufdecken kann. Ein erfolgloser Eindringversuch zeigt nur, dass das System gegen diesen einen speziellen Angriffsversuch immun war. Ein neuer Versuch mit anderen Methoden könnte jedoch erfolgreich sein. Nicht zu unterschätzen sind auch die negativen psychologischen Auswirkungen auf die Administratoren der angegriffenen Systeme, die den Penetrationstest als Misstrauensvotum interpretieren könnten. Die Möglichkeiten eines Angriffes sind umfassend und komplex. Die Kontrollen gelten den grundlegenden Massnahmen, die den Aufwand für die erfolgreiche Attacke eines potenziellen Angreifers wesentlich erhöhen.

Vorgehen

Das beschriebene Vorgehen überprüft, ob die folgenden typischen Angriffe abgewehrt werden können und keine unnötigen Internetdienste in Betrieb sind:

- Versuch, in das interne Netzwerk einzudringen, mit dem Ziel, Daten zu lesen, zu verändern, zu stehlen oder gar zu löschen.
- Versuch, die Konfiguration von Schutzeinrichtungen derart zu verändern, dass die Schutzwirkung deaktiviert oder vermindert wird.
- Versuch, die Verfügbarkeit der betriebs-eigenen Informatikmittel zu beeinträchtigen.

Die Angriffe werden in der Regel von «ausser», also vom Internet her, durchgeführt, um so Zugriff auf Routers, Firewalls, Server und PC zu erhalten.

Die Vorgehensweise zur Durchführung eines Penetrationstests sollte nach folgendem Modell erfolgen:

1. Recherche nach Informationen über das Zielsystem

Im Internet erreichbare Rechner müssen über eine offizielle IP-Adresse verfügen. Frei zugängliche Datenbanken liefern Informationen über IP-Adressblöcke, die einer Organisation zugewiesen sind. Feststellen der registrierten Domains, IP-Adressen und zuständigen Personen:

- www.switch.ch
- www.networksolutions.com
- www.netcraft.com

Whois-Datenbanken:

- www.ripe.net (Europa)
- www.arin.net (Amerikanischer Kontinent)
- www.apnic.net (Asiatisch/Pazifischer Raum)

2. Scan der Zielsysteme auf angebotene Dienste

Hierbei wird versucht, den oder die zu überprüfenden Rechner einem sog. Portscan zu unterziehen, wobei evtl. geöffnete Ports Rückschlüsse auf die zugeordneten Anwendungen zulassen.

3. System- und Anwendungserkennung

Über das sog. «Fingerprinting» können Namen und Version von Betriebssystemen und Anwendungen auf den Zielsystemen in Erfahrung gebracht werden.

4. Recherche nach Schwachstellen

Anhand der gewonnenen Informationen können zielgerichtet Informationen über Schwachstellen bestimmter Betriebssysteme und Anwendungen gesucht werden.

5. Ausnutzen der Schwachstellen

Gefundene Schwachstellen können dazu genutzt werden, unberechtigten Zugriff zum System zu erhalten bzw. weitere Angriffe vorzubereiten.

Qualität und Nutzen eines Penetrationstests hängt im Wesentlichen davon ab, inwieweit er auf die individuelle Situation des Auftraggebers eingeht, d.h. wie viel Zeit und Ressourcen der Dienstleister auf die Ausforschung von Schwachstellen, die die konkrete IT-Infrastruktur betreffen, verwendet und wie kreativ er dabei vor-

geht. Dieser Ablauf kann nicht mehr in der obigen allgemein gültigen Beschreibung dargestellt werden. Deshalb existieren grosse Unterschiede bezüglich der Qualität der als Penetrationstest bezeichneten Dienstleistung.

Folgende Kontrollen werden durchgeführt:

- Einsehbarkeit von Information über die Internetverbindung eines Unternehmens
- Offene Datenkanäle (Ports) ins interne Netz
- Zugriff auf Routers und Firewalls
- Zugriff auf interne Server-Dienste
- Denial-Of-Service-Attacke (ein System deaktivieren)
- Kontrolle organisatorischer Massnahmen
- Funktionen der Alarmmechanismen? (Wie wird reagiert?)
- Sensibilisierung der Verantwortlichen und des Managements

Die erläuterten «Angriffe» können die Funktion der Internetverbindung beeinträchtigen oder sogar zum Ausfall einzelner Komponenten führen. Die Tests müssen deshalb unbedingt in Absprache mit den verantwortlichen Stellen der Unter-

nehmung durchgeführt werden. Eine schriftliche Bewilligung kann vor allfälligen Schadenersatzansprüchen schützen.

Durchführung

Eine erfolgreiche Durchführung des Penetrationstests, die den Erwartungen des Auftraggebers entspricht, bedingt eine klare Zielvereinbarung. Falls Ziele angestrebt werden, die nicht bzw. nicht effizient erreicht werden können, so sollte der Tester in der Vorbereitungsphase deutlich darauf hinweisen und alternative Vorgehensweisen wie z. B. eine IT-Revision oder IT-Sicherheitsberatung empfehlen.

Um die oben erwähnten «Angriffe» auf das eigene Netzwerk durchführen zu können, werden folgende Elemente benötigt:

- Grundlegende IT- und TCP/IP-Kenntnisse
- Zugang zu einem externen PC, der über eine direkte Verbindung zum Internet verfügt (nicht über das firmeninterne Netzwerk)
- Entsprechende Software, um die Tests durchführen zu können

- Genaue Definition der Ziele
- Genaue Planung des Tests und Besprechung mit den involvierten Personen
- Notfallprozedere bereitstellen
- Protokollierung des Penetrationstests (revisionsfähig)
- Daten sind vertraulich zu behandeln
- Detaillierter Abschlussbericht mit möglichen Massnahmen

Die Ziele des Auftraggebers, die mit einem Penetrationstest erreicht werden können, lassen sich in vier Gruppen einteilen:

1. Erhöhung der Sicherheit technischen Systeme
2. Identifikation von Schwachstellen
3. Bestätigung der IT-Sicherheit durch einen externen Dritten
4. Erhöhung der Sicherheit der organisatorischen und personellen Infrastruktur

Im Ergebnis des Tests sollten daher nicht nur eine Liste vorhandener Schwachstellen, sondern auch konkrete Lösungsvorschläge für deren Beseitigung aufgeführt werden. ■