

Angriff ist die beste Verteidigung

Kontrollierte Attacken aus dem Internet

Abstract

Einige Netzwerkingenieure sagen: "Es gibt nur eine Möglichkeit die Sicherheit von Computersystemen zu gewährleisten, indem zwischen dem Netzwerk und jedem Computer ein Luftzwischenraum von zehn Zentimetern besteht!" Doch welche Vorkehrungen können getroffen werden, wenn diese Option nicht befriedigend ist?

Grundsätzliches über Attacken

Attacken richten sich gegen alle Arten von Diensten und Daten, die über eine physische Verbindung zum Internet angesprochen werden könnten. Wenn eine physische Verbindung besteht, ist das Ziel einer Attacke, die möglicherweise vorhandenen logischen Barrieren zu durchbrechen oder zu umgehen.

Eine Attacke läuft meistens in drei Phasen ab:

Phase I

In der ersten Phase geht es darum, sich Zugriff zum System zu verschaffen. Das erste Ziel bei einer Attacke auf ein UNIX- oder NT-System wird sein, sich einen Loginaccount und ein Passwort zu beschaffen. Der Hacker wird versuchen, eine Kopie der Passwortdatei zu bekommen. In dieser Datei wird die Zuordnung von jedem Benutzer mit seinem Passwort gemacht. Die Passwörter sind chiffriert in dieser Datei aufgeführt.

Wenn jemand eine solche Passwortdatei besitzt, kann er mit entsprechenden Programmen versuchen, einzelne Passwörter zu knacken. Solche Programme greifen auf elektronische Lexika zu, chiffrieren einen Lexikoneintrag und vergleichen ihn mit dem chiffrierten Eintrag in der Passwortdatei.

Aus diesem Grund ist es wichtig, schwierige Passwörter zu wählen, die Ziffern und Sonderzeichen enthalten.

Um nun einen Loginaccount der zu attackierenden Unternehmung zu erhalten, sammelt ein Hacker Informationen über Sicherheitslücken in den eingesetzten Softwareprodukten, sowie Möglichkeiten, diese auszunützen. Des weiteren verschafft er sich einen Überblick über das Netzwerk und die eingesetzten Systeme des zu attackierenden Unternehmens. Die Kombination dieser Informationen wird in vielen Fällen vorhandene Hintertüren aufzeigen und bildet somit die Angriffsbasis. Ein Hacker braucht nur eine Sicherheitslücke in einem ganzen Netzwerk, um unerlaubten Zugriff zu erhalten.

Phase II

In der zweiten Phase versucht der Eindringling, seine Zugriffsrechte zu erweitern, zum Beispiel durch Ausnützen von Programmen, die unter UNIX mit privilegiertem Status laufen.

Dies kann ihm die Sonderstellung eines Administrators geben. Mit diesem Status hat er uneingeschränkten Zugriff auf alle Daten im System. Zusätzlich kann er alle seine Spuren verwischen, womit es für reguläre Administratoren unmöglich wird, die Präsenz eines Hackers nachzuweisen.

Die Möglichkeiten, die für einen Hacker in dieser Phase bestehen, können stark eingeschränkt werden, indem sogenannte "Sicherheitspatches" für Programme und das Betriebssystem installiert werden. Es empfiehlt sich sehr, auch die Empfehlungen des "Computer Emergency Response Team" (CERT) zu implementieren. Ausserdem ist auf eine gute Qualität bei der Systemadministration zu achten.

Phase III

Das Ziel der dritten Phase wird sein, von dem erfolgreich attackierten System aus, Zugriff zu weiteren Systemen im Netzwerk zu haben.

Sollte ein Hacker in diese Phase vorgedrungen sein, drohen der Unternehmung aufwendige Neuinstallationen von Betriebssystem und Programmen. Längere Unterbrüche, unzufriedene Kunden und frustrierte Mitarbeiter sind die Folgen. Die finanziellen Auswirkungen und der Imageverlust eines Unternehmens hängen ab von der Art und Weise der Attacke sowie vom Sicherheitslevel des angegriffenen Netzwerkes.

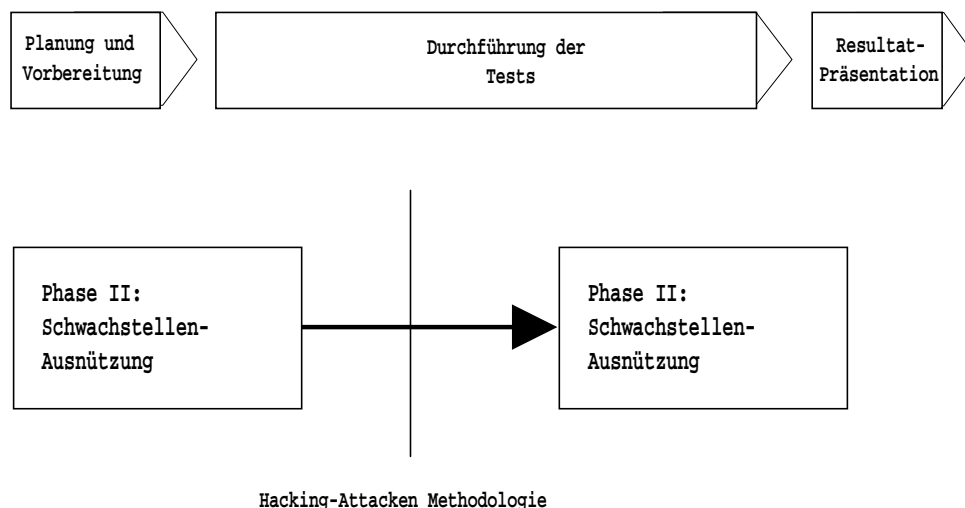
Abwehren einer Attacke

Welche Möglichkeiten hat nun ein Unternehmen, um die Sicherheit seines Netzwerkes zu verbessern? Hier muss unterschieden werden, ob es sich um die innere Sicherheit oder die gegen aussen handelt.

Die innere Sicherheit sollte entlang einer Sicherheitspolitik definiert und umgesetzt werden. Verschiedene Risikobereiche wie Informationen, Systemressourcen, Netzwerkkomponenten sowie die Administration und Wartung, sollten einer ständigen Kontrolle und Verbesserung unterliegen. Die Qualität der internen Sicherheit begrenzt den möglichen Schaden, der bei der Überwindung äusserer Barrieren angerichtet werden kann.

Die äussere Sicherheit wird bestimmt durch Firewalls oder andere kontrollierte Zugangspunkte zum privaten Netzwerk. Um die Sicherheit dieser Zugänge zu testen, empfiehlt es sich, eine Hacking-Attacke durch eine externe Organisation vornehmen zu lassen. Bei einer solchen legalen Attacke werden Aussagen nicht nur über die Sicherheit einer Firewallimplementation gemacht, sondern auch darüber, wie effektiv eine Sicherheitspolitik in die Tat umgesetzt wurde, wie gut das private Netzwerk implementiert ist und administriert wird oder wie mit den Risiken umgegangen wird.

Wir z.B. führen solche Hacking-Attacken mit Hilfe einer eigens von uns entwickelten Methodologie durch. Diese lässt sich stark vereinfacht wie folgt darstellen:



Wichtig bei solchen Hacking-Attacken ist einerseits das methodische Vorgehen bei der Durchführung und andererseits die Abdeckung eines breiten Spektrums von technischen Schwachstellen. Organisatorische Aspekte sowie wichtige Elemente des Technologie Management sind wesentliche Bestandteile dieser systematischen Vorgehensweise.

Zusammenfassend lässt sich sagen, dass die zunehmende Komplexität der Systeme und Netzwerke zu immer neuen potentiellen Schwachstellen führt.

Um Hackern einen ernsthaften Widerstand bieten zu können, sind laufend Aufwände zur Verbesserung der Sicherheit notwendig. Gezielte und kontrollierte Attacken sollten ein Bestandteil dessen sein.

Literaturverzeichnis

- [VERD97] Denis Verdon. (1997): Penetration test methodology. Price Waterhouse; London UK.
- [ESF96] Members of the European Security Forum. (1996): THE INTERNET AND SECURITY. European Security Forum (ESF); London UK.
- [ISPR96] Derek Atkins, Paul Buis, Chris Hare, Robert Kelly, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, William Steen. (1996): INTERNET SECURITY PROFESSIONAL REFERENCE. New Riders Publishing; Indianapolis US.

Roger Auinger, dipl. Ing. HTL, Consultant, ist Mitarbeiter von Information Systems Risk Management (ISRM) der Revisuisse Price Waterhouse AG in Zürich, und leitet dort das Internet-Security Team.