

## Penetrationstest – Ist Ihre Sicherheit wasserdicht?

Ein Anschluss des Unternehmensnetzes an das Internet ist heute gängiger Standard. Internet-Dienste wie WWW, Mail, oder Remote-Zugang, etc. sind für die meisten Organisationen kaum mehr wegzudenken. Mit der Verbindung zum Internet als öffentlichem und damit unsicherem Netzwerk sind verschiedene Risiken verbunden. Durch den zweckmässigen Einsatz der entsprechenden technischen Mittel wie Firewalls, Proxies, Adressübersetzungen, etc. und das Einhalten von Richtlinien im Umgang mit den Internet-Diensten können die Risiken auf ein vertretbares Mass reduziert werden. Um eine permanente Sicherheit zu gewährleisten, sollten die technischen wie auch die organisatorischen Massnahmen regelmässig überprüft werden. Mit der nachfolgenden Anleitung können die Einstellungen der exponierten Systeme kontrolliert und grobe Fehler frühzeitig erkannt werden.



### W. Sidler

Nachdiplom FH Informatik Sicherheit, eidg. Wirtschaftsinformatiker und Mitautor des «Sicherheitshandbuches für die Praxis»  
[www.sihb.ch](http://www.sihb.ch)

Die Sicherheit jener Systeme, die über Verbindungen zu öffentlichen Netzen verfügen, unterliegen in besonderer Weise unautorisierten, meist anonymen Zugriffsversuchen. In dieser Situation werden Testmethoden benötigt, die sich des

Blickwinkels der Angreifer bedienen, um möglichst reale Testbedingungen schaffen zu können. Im technischen Sprachgebrauch versteht man unter einem **Penetrationstest** den kontrollierten Versuch, von „ausser“ in ein bestimmtes Computersystem bzw. Netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden die gleichen Techniken eingesetzt, die auch bei einem realen Angriff verwendet werden. Die hierbei identifizierten Schwachstellen können dann durch entsprechende Massnahmen behoben werden, bevor diese von unautorisierten Dritten genutzt werden können.

#### Täterprofile

Üblicherweise wird in der medialen Berichterstattung unter dem Begriff „Hacker“ pauschal eine Person bezeichnet, die 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. 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 verfügen, die sie angreifen wol-

len, werden als Insider bezeichnet. Oft handelt es sich bei Insidern um frustrierte (ehemalige) Mitarbeiter einer Organisation, die ihr erworbenes Wissen über betriebsinterne Sachverhalte dazu nutzen, der Organisation Schaden zuzufügen. Die Gefahr, die von Insidern ausgeht, ist dabei 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: Ziel der Wirtschaftsspionage ist es, von Betriebsgeheimnissen wie innovativen technischen Konzepten, Strategien und Ideen, die einen Wettbewerbsvorteil bedeuten, Kenntnis zu erlangen und zum eigenen Vorteil zu verwenden.

### **Vorgehensweise der Täter**

Es existieren mehrere Möglichkeiten, IT-Systeme in ihrer Funktionsweise zu manipulieren oder zu schädigen bzw. einen Angriff auf IT-Systeme vorzubereiten. Unter „Angriffe über das Netzwerk“ versteht man Attacken, die unter der Nutzung von Funktionalitäten der eingesetzten Netzwerkprotokolle auf Netzwerkkomponenten, Computersysteme und/oder Applikationen stattfinden. Diese Art von Angriffen macht sich Schwachstellen oder Unzulänglichkeiten in Hard- und Software zunutze, um Angriffe vorzubereiten oder durchzuführen. Mögliche Arten von Angriffen 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 privilegiertem Wissen insofern zu manipulieren, dass sie dem Angreifer sicherheitsrelevante Informationen, wie z. B. Passwörter, preisgeben. Beispielsweise könnte sich ein Angreifer als IT-Mitarbeiter einer Organisation ausgeben und dadurch einen arglosen Benutzer unter einem Vorwand zur Herausgabe seines Netzwerk-Passwortes bewegen. Besonders bei dieser Technik 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 Grundvoraussetzung zur Gewährleistung von IT-Sicherheit. Wenn physische Sicherheitsmassnahmen überwunden werden können und auf diese Weise physischer Zugriff auf die IT-Systeme 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. Ein Beispiel ist das unbefugte Eindringen in das Rechenzentrum einer Organisation und das Entwenden einer Festplatte mit vertraulichen Daten. Auch das Durchsuchen von Abfällen nach Dokumenten mit sicherheitssensitiven Informationen (Dumpster Diving) gehört zu dieser Gruppe.

### **Der Penetrationstest**

Der Begriff „Penetrationstest“ und die dazu durchgeführten Methoden wurden 1995 etabliert, als der erste Unix-basierte Schwachstellen-Scanner „SATAN“ [Venema95] veröffentlicht wurde. Das Programm stellte zur damaligen Zeit das erste Tool dar, das automatisiert Rechner auf Schwachstellen untersuchen konnte.

Unter einem so genannten Penetrationstest versteht man den Versuch, autorisiert in ein Netzwerk einzubrechen, um Aufschluss über dessen Sicherheitsniveau zu erhalten. Ziel eines solchen Penetrationstests könnten zum Beispiel eine Firewall, ein Mail-, Web- oder Datenbankserver, Applikationen oder das ganze Netz sein. Von äusserster Wichtigkeit ist jedoch die Tatsache, dass ein Penetrationstest nur teilweise vorhandene Schwachstellen aufdecken kann. Auch 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, welche den Penetrationstest als Misstrauensvotum interpretieren könnten.

Die Möglichkeiten eines Angriffes sind umfassend und komplex. Die Kontrollen gelten den grundlegenden Massnahmen, die den Aufwand für eine erfolgreiche Attacke eines potentiellen Angreifers wesentlich erhöhen.

### **Vorgehen**

Durch das beschriebene Vorgehen kann überprüft werden, ob

## PLATTFORM FÜR INFORMATIONSSICHERHEIT

die folgenden typischen Angriffe abgewehrt werden können und keine unnötigen Internet-Dienste 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 betriebseigenen Informatikmittel zu beeinträchtigen

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

Die Vorgehensweise zur Durchführung eines Penetrationstests sollte nach dem folgenden Vorgehensmodell durchgeführt werden:

### 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](http://www.switch.ch)

[www.networksolutions.com](http://www.networksolutions.com)

[www.netcraft.com](http://www.netcraft.com)

Whois-Datenbanken:

[www.ripe.net](http://www.ripe.net) (Europa)

[www.arin.net](http://www.arin.net) (Amerikanischer Kontinent)

[www.apnic.net](http://www.apnic.net) (Asiatischer und 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 sich 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.

Die Qualität und der Nutzen eines Penetrationstests werden im Wesentlichen davon bestimmt, inwieweit dieser 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 vorgeht. 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 Internet-Verbindung 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 Internet-Verbindung beeinträchtigen oder sogar zum Ausfall einzelner Komponenten führen. Die Tests müssen deshalb unbedingt in Absprache mit den verantwortlichen Stellen der Unternehmung durchgeführt werden. Eine schriftliche Bewilligung kann vor allfälligen Schadenersatzansprüchen schützen.

### Durchführung

Für eine erfolgreiche Durchführung eines Penetrationstests, die den Erwartungen des Auftraggebers entspricht, ist eine klare Zielvereinbarung unbedingt notwendig. 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.

## PLATTFORM FÜR INFORMATIONSSICHERHEIT

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, welcher 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 der 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 eines IT-Penetrationstests sollte daher nicht nur eine Auflistung vorhandener Schwachstellen vorhanden sein, sondern möglichst auch konkrete Lösungsvorschläge für deren Beseitigung aufgeführt werden.

Im Folgenden werden die vier Zielgruppen anhand von konkreten Beispielen erläutert.

### **Erhöhung der Sicherheit der technischen Systeme**

Die meisten Penetrationstests werden mit der Zielsetzung in Auftrag gegeben, die Sicherheit der technischen Systeme zu erhöhen. Die Tests beschränken sich auf die technischen Systeme, wie Firewall, Router, Web-Server, etc., die organisatorische bzw. personelle Infrastruktur wird nicht explizit geprüft. Ein Beispiel ist ein Penetrationstest, bei dem gezielt geprüft werden soll, ob es unautorisierten Dritten möglich ist, über das Internet auf Systeme innerhalb des LANs des Unternehmens zuzugreifen. Mögliche Ergebnisse bzw. Feststellungen des Tests sind nicht benötigte offene Ports der Firewall, verwundbare Versionen der eingesetzten Internet-Applikationen, Betriebssysteme.

### **Identifikation von Schwachstellen**

Im Unterschied zu den anderen drei Zielen ist die Identifikation hier als Entscheidungskriterium das direkte Ziel des Tests. So kann beispielsweise vor dem Zusammenschalten zweier LANs im Rahmen eines Firmenzusammenschlusses geprüft werden, ob es möglich ist, in das neue LAN von aussen einzudringen. Falls dies durch den Penetrationstest gelingt, müssen vor dem Zusammenschluss Massnahmen zur Sicherung des Übergangs getroffen werden oder sogar vom Zusammenschluss generell Abstand genommen werden.

### **Bestätigung der IT-Sicherheit durch einen externen Dritten**

Ein Penetrationstest kann auch durchgeführt werden, um eine Bestätigung eines unabhängigen, externen Dritten zu erlangen. Dabei sollte beachtet werden, dass ein Penetrationstest immer nur eine Momentaufnahme darstellt und daher keine Aussagen über das Sicherheitsniveau für die Zukunft gegeben werden kann. Dennoch kann z. B. die regelmässige Durchführung von Penetrationstests geeignet sein, um eine erhöhte Sicherheit der Kundendaten innerhalb eines Webshops oder einer anderen Internet-Applikation zu demonstrieren.

### **Erhöhung der Sicherheit der organisatorischen / personellen Infrastruktur**

Neben der technischen Infrastruktur kann ein Penetrationstest auch die organisatorische/personelle Infrastruktur, beispielsweise zur Kontrolle von Eskalationsprozeduren, prüfen. Dazu kann stufenweise der Umfang bzw. die Aggressivität des Tests gesteigert werden. Mittels Social-Engineering-Techniken, wie z. B. mit telefonischen Abfragen von Passwörtern, kann das allgemeine Bewusstsein bzw. die Wirksamkeit von Sicherheitsleitlinien und Nutzungsvereinbarungen evaluiert werden.

### **Checkliste**

- ✓ Schriftliche Form (Vertrag) mit dem Dienstleistungserbringer
- ✓ Genaue Beschreibung von Ziel, Verfahren, eingesetzte Technologien
- ✓ Vertraulichkeitserklärung

---

## PLATTFORM FÜR INFORMATIONSSICHERHEIT

- ✓ Einverständniserklärung für einen Penetrationstest
- ✓ Genaue Zeitplanung
- ✓ Verhindern, dass produktive Systeme während den Geschäftszeiten beeinträchtigt werden
- ✓ Mögliche Risiken und deren Auswirkungen kennen
- ✓ Abbruchkriterien definieren (Notfallplanung)
- ✓ Inhalt des Abschlussberichtes definieren
- ✓ Bereitstellen der notwendigen System- und Netzwerk-Dokumente (Konfigurationen)

Information von möglicherweise betroffenen Dritten