

## IT-Sicherheitsüberprüfungen heute



Viele Firmen haben in den letzten Jahren den Bedarf für IT-Sicherheit erkannt und nicht unerhebliche Summen in den Aufbau einer Infrastruktur zum Schutz ihrer Netze und Daten investiert. Dennoch liest man regelmäßig neue Meldungen über erfolgreiche Einbrüche oder Datendiebstahl. Offenbar reichen in vielen Fällen auch Firewalls und Intrusion Detection Systeme für mehrere hunderttausend Euro nicht aus, um Hacker dauerhaft fern zu halten.

cirosec GmbH  
Jörg-Ratgeb-Platz 3  
74081 Heilbronn  
Tel.: 07131 / 59455-60  
Fax: 07131 / 59455-99  
[www.cirosec.de](http://www.cirosec.de)

Als Ursache für diese Situation kommen unterschiedliche Faktoren in Frage. Einerseits werden nicht immer die richtigen Technologien zum Schutz verwendet, beispielsweise können Firewalls meist nichts gegen Angriffe auf der Anwendungsebene bewirken, andererseits sind auch bei korrekter Auswahl der Technologien und Produkte häufig starke Defizite bei der konkreten Implementation und Konfiguration erkennbar. Nicht zuletzt muss sich der Sicherheitsanspruch auch in der Organisation und dem Betrieb niederschlagen, damit überhaupt ein vernünftiges Sicherheitsniveau erreicht wird.

Um Fehler in diesen Bereichen frühzeitig erkennen zu können, bieten viele Beratungsfirmen eine Überprüfung der Sicherheit an, bei deren Abschluss eine Bewertung und eine Mängelliste vorgelegt werden. Dabei betrachten die Berater je nach Art der Prüfung die konkrete technische Umsetzung, die organisatorischen Prozesse oder auch das Gesamtkonzept. Häufig werden auch so genannte „Penetration Tests“ durchgeführt, bei denen der Berater versucht, tatsächlich in ein geschütztes System einzudringen und damit den Beweis der Unsicherheit zu liefern.

In jedem Fall ist die Erfahrung und das Wissen der Berater der entscheidende Faktor für die Aussagekraft einer solchen Überprüfung, denn die Sicherheitslücken, die einen Einbruch ermöglichen, sind häufig klein und versteckt. Nur mit genügend Wissen über die Arbeitsweise eines Hackers, seine Werkzeuge und Tricks kann man diese Lücken finden und ihre Bedeutung bewerten.

Dieses Know-how ist jedoch einer sehr kurzen Halbwertszeit unterworfen. Ständig kommen neue Produkte auf den Markt, die neue Fehler und Verwundbarkeiten mit sich bringen und ständig entwickeln einzelne Hacker oder Gruppen neue Angriffswerkzeuge. In diesem Bereich ständig auf dem Laufenden zu bleiben ist eine große Herausforderung.

Auf dem Markt werden verschiedene Sicherheitsüberprüfungen angeboten, die sich aufgrund der folgenden Kriterien unterscheiden können:

- Standort des Prüfers
  - Vor-Ort-Überprüfung
  - Überprüfung über externe Netze
- Kenntnisse des Prüfers vor Untersuchungsbeginn
  - Netzwerkstruktur
  - Konfigurationsdetails wie Firewall-Regeln oder ähnliches
  - Keine Kenntnisse
- Zugangsberechtigungen
  - Zugang zu wichtigen Servern und Prüfung ihrer Konfiguration mit Administratorrechten
  - Keine Zugangsberechtigungen

- Zu untersuchende Aspekte
  - Technische Implementation
  - Konfiguration
  - Organisation
  - Betrieb
  
- Zu untersuchende Zugangsmechanismen
  - Internet
  - ISDN
  - Modems
  - WLANs
  
- Tiefe der Prüfung
  - Bis zum Verdacht eines Fehlers
  - Vollständigen Ausnutzung und evt. auch DoS

Die wohl am häufigsten angebotene und durchgeführte Art einer Sicherheitsüberprüfung ist der toolgestützte, externe Scan. Dabei kommt der Prüfer nicht zum Kunden, sondern er lässt die extern erreichbaren IP-Adressen des Kunden mit einem automatischen Werkzeug wie beispielsweise dem Internet-Scanner von ISS oder mit Nessus aus dem Open Source-Umfeld analysieren. Die Ausgabe dieses Werkzeugs wird dann häufig umformatiert, mit Kommentaren versehen und dem Kunden als Ergebnis vorgelegt. Diese Variante ist nicht nur die häufigste, sondern auch die kostengünstigste und sicherlich aber auch die oberflächlichste Überprüfung. Sie reicht aus, um offensichtliche Fehler zu entdecken, geht jedoch nicht sehr in die Tiefe. So ist es sehr unwahrscheinlich, verborgene Fehler zu finden oder auch Fehler in Web-Applikationen auf Anwendungsebene zu entdecken.

Als innovative und wichtige Variation der externen Scans gibt es Scan-Werkzeuge, die speziell auch nach Fehlern in der Anwendungsebene suchen oder generische Hacker-Methoden integrieren. Auf diese Weise sind Sicherheitslücken auffindbar, die sonst nur durch eine Source Code-Analyse entdeckt werden.

Die deutlich teurere Art der Überprüfung ist die Vor-Ort-Überprüfung. Dabei wird das Netz des Kunden nicht nur aus der Entfernung betrachtet, sondern auch die Installation und Konfiguration der einzelnen Komponenten vor Ort. Dazu kommt der Prüfer zum Kunden und benötigt Einblick in die Details möglichst vieler Geräte.

Die Aussagekraft dieser Art von Prüfungen ist deutlich höher als die eines externen Scans, da auch strukturelle Schwachstellen aufgezeigt werden können, die bei einem Scan noch gar nicht sichtbar werden.

Bei eher technisch orientierten Beratungsfirmen wird auch gerne ein vollständiger „Penetration Test“ angeboten. In diesem Fall versucht der Prüfer gefundene Schwachstellen auch auszunutzen und damit das Problem zu beweisen. Diese Art der Untersuchung ist zwar spektakulär, jedoch hilft sie dem Kunden aufgrund der begrenzten Zeit nicht sehr viel weiter. Die Sicherheitslücken, die bei einem erfolgreichen Einbruch ausgenutzt werden, sind meist schon bei einem externen Scan, auf jeden Fall aber bei einer detaillierten Vor-Ort-Analyse sichtbar. Versteckte Schwachstellen dagegen können in der begrenzten Zeit eines Penetration Tests meist gar nicht gefunden werden.

Besonders große Beratungsfirmen untersuchen mit Vorliebe nicht nur die technischen Schwachstellen, sondern auch die Betriebskonzepte und Policies. Dafür ist mehr organisatorisches Know-how und weniger technisches Detailwissen gefragt. In den allermeisten Fällen findet man bei der Organisation und bei der Überwachung von Sicherheitsmechanismen genügend Schwachstellen.

Ein generelles Problem bei allen bisher beschriebenen Überprüfungsarten ist, dass es nur einzelne Momentaufnahmen sind. Jegliche Aussage über Sicherheit – von offensichtlichen Problemen abgesehen – hat nur eine sehr kurze Zeit Gültigkeit, da sich schon nach wenigen Tagen neue Fehler einschleichen können und ständig neue Fehler in Softwareprodukten bekannt werden.

Das Problem der Aktualität kann durch automatisierte Scanning-Services behoben werden, die täglich aufs Neue und mit ständig aktualisierten Prüfungen die Infrastruktur analysieren.

Zusätzlich zu den externen Services gibt es interessante neue Technologien auf dem Markt, die ein System von innen scannen. Auf diese Weise werden viele zusätzliche Schwachstellen gefunden, da auch die Systemkomponenten überprüft werden können, die von außen nicht erreichbar sind.

Natürlich sind dabei keine besonders tief gehenden Prüfungen möglich, aber alleine schon die ständige Aktualität und tägliche Durchführung bieten einen großen Vorteil gegenüber Prüfungen, die nur einmal im Jahr oder alle 3 Monate durchgeführt werden. Da die meisten Anbieter auch einen Differenz-Report zur Verfügung stellen, in dem nur neu hinzugekommene Probleme und die Gesamtbewertung dargestellt werden, muss der Report nicht jedes Mal vollständig gelesen werden.

Zusammenfassend ist festzuhalten, dass die automatisierten Scanning-Services nur das Problem der Aktualität lösen, tief gehende Sicherheitsüberprüfungen durch Berater aber nicht ersetzen können.



cirosec GmbH  
Jörg-Ratgeb-Platz 3  
74081 Heilbronn  
Tel.: 07131 / 59455-60  
Fax: 07131 / 59455-99  
[www.cirosec.de](http://www.cirosec.de)