

SySS-Workshop: Planung und Durchführung von Penetrationstests

IT-Security ist in aller Munde. Die Tatsache, dass eine unsichere IT-Landschaft den Betrieb oder sogar den Fortbestand von Unternehmen gefährden kann, wird immer offensichtlicher. Meist reißen kleine, unscheinbare Fehler gefährliche Löcher in IT-Netze. Voraussetzung für das Beheben dieser Fehler ist, diese kennenzulernen.

IT-Infrastrukturen und Applikationen können hochwertig und robust konzipiert sein und dennoch Lücken aufweisen. Um Schwachstellen auf die Spur zu kommen, eignet sich der Penetrationstest hervorragend als Kontrollinstrument. Denn auf diese Weise können IT-Netze von außen und innen auf Schwachstellen hin untersucht werden.

Die Durchführung solcher simulierter Hacker-Attacken ist aber alles andere als einfach und wird im Workshop diskutiert:

- Warum PenTests?
- Gegenstand der Prüfungen (Perimeter, LAN, WLAN, Web-Applikationen,...)
- Gestaltungsmöglichkeiten:
 - Angekündigt / unangekündigt?
 - Einmalig oder als Prozess?
 - Blackbox- oder Whitebox-Test?
 - Durch einen externen Experten oder intern?
 - Aggressive oder vorsichtige Vorgehensweise?
- Kosten-/Nutzenverhältnis
- Vorgehensweise
- Projektmanagement
- Nachverfolgung von Schwachstellen
- Politische Folgen innerhalb des Unternehmens
- Ethische Aspekte



Referent: Dipl.-Inform. Sebastian Schreiber (SySS GmbH)

- 1993-1999 Studium der Informatik, Physik, Mathematik und BWL an der Eberhard Karls Universität Tübingen
- 1996-1998 Mitarbeiter bei Hewlett-Packard, 1996 MicroGold (USA)
- 1998-heute Geschäftsführer der SySS GmbH (Penetrationstests bei einer Vielzahl von Unternehmen)
- Zahlreiche Veröffentlichungen, Vorträge im In- und Ausland; Mitherausgeber der IT-Sicherheit und Datenschutz