

Agenda: Gestaltungsmöglichkeiten von Penetrationstests

IT-Security ist in aller Munde. Dass die Gefährdung der IT-Landschaft den Betrieb oder sogar den Fortbestand eines Unternehmens gefährden kann wird immer offensichtlicher. Meist reißen kleine, unscheinbare Fehler gefährliche Löcher in IT-Netze. Voraussetzung für das Beheben dieser Fehler ist, diese zu kennen.

Ein effektiver Ansatz hierzu stellen Penetrationstests dar. Von außen und innen werden die IT-Netze auf Schwachstellen hin untersucht. Die Durchführung solcher simulierter Hacker-Attacken ist aber alles andere als einfach und wird im Vortrag 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 der Schwachstellen
- Politische Folgen innerhalb des Unternehmens
- Ethische Aspekte



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

- 1993-1999 Studium von 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