AMC-Business-Training

Hacker-Attacken

IT-Sicherheitstraining für AMC-Versicherungsunternehmen und AMC-Kooperationspartner

17. September 2009, 9:45 - 17:00 Uhr, Marriott Hotel, Johannisstraße 76 - 80, 50668 Köln

Top

1 Begrüßung, Vorstellung Referent und Teilnehmer — 09:45

Andreas Wölker, AMC Münster

2 Hacker-Attacken — 10:00

Martin G. Wundram, Dormagen

Vereidigter Sachverständiger für Computerforensik und –sicherheit

Teil 1

- Einführung, Problembewusstsein, Probleme und Gefahren im Bereich der IT
  - Gefährdungsfaktoren, Angreifertypen
  - Kosten-/Nutzenabschätzung für Sicherheitsmaßnahmen
  - Bedrohungsszenarien
    - Angriffe gegen Nutzer vs. Angriffe gegen Server/Anbieter
  - Beispiele gehackter Webseiten
- Ausspähen der Infrastruktur
  - Techniken, um eine Netzwerkinfrastruktur und
  - die Infrastruktur einer Webseite aus Sicht eines Angreifers zu analysieren
- Abfangen von Daten und Hinleitung zu Phishing
  - Techniken, um in einem LAN und über das Internet Daten Dritter per Man-In-The-Middle- und Phishing-Angriffen abzufangen (Klartext und HTTPS)

Gemeinsames Mittagsessen — 12:00

Teil 2 — 13:30

- Betriebssysteme kompromittieren
  - Kontrolle gewinnen über einen unixoiden Server über eine Schwachstelle in dessen Webapplikation
- Authentifizierungssysteme
  - POP-E-Mail-Account hacken, versteckte Protokollierung vertraulicher Daten
- Web-Security
  - Häufige Fehler, Maßnahmen zur Vermeidung, Auswahl von Angriffstechniken: Cross-Site-Scripting, Cross-Site-RequestForgery/Session-Riding, SQL-Injection, Mailheader-Injection

Pause — 15:30

Teil 3 — 16:00

- W-LAN-Hacking
  - Kurze Betrachtung der Theorie, Angriff auf ein WEPverschlüsseltes Netzwerk, Ausblick auf Technik WPAlWPA2
- Kommerzialisierung
- Social Engineering

ca. Ende des Workshops — 17:00

Stand 15.07.2009 - Änderungen vorbehalten