

Wireless LAN – Hacking und Wardriving

Die Sicherheit drahtloser Netzwerke auf dem Prüfstand

Nicht nur die Werbekampagnen der großen Internet Service Provider haben zu einer stetig wachsenden Verbreitung von Wireless LANs geführt, sondern auch die Vorteile der Funknetze überzeugen immer mehr Unternehmen vom lohnenswerten Einsatz dieser Technologie. Gerade die Flexibilität und die gesparten Kosten für die Netzwerkinfrastruktur sind dabei die bedeutendsten Pluspunkte.

Mit einer stetig wachsenden Verbreitung interessieren sich aber auch immer mehr Außenstehende für fremde Funknetze. Dieses Interesse kann rein sportlicher Natur sein, wie im Falle des Wardriving, aber auch eine Bedrohung für den Betreiber des Wireless LAN, wenn es als Plattform für einen Angriff auf die IT-Infrastruktur genutzt wird. Noch immer werden viele WLANs vollkommen ungesichert oder nur unzureichend geschützt betrieben.

Lernen sie in diesem Training die Technik der WLANs kennen, unternehmen sie die ersten Schritte zur Absicherung und überprüfen sie den Erfolg ihrer Schutzmaßnahmen. Danach werden typische Angriffe auf Funknetze erläutert und demonstriert. Mit diesem Wissen werden sie sich dann aktuelleren Authentisierungs- und Verschlüsselungsmaßnahmen zuwenden um ihr Wireless LAN vor ungebetenen Besuchern zu schützen.

Daneben werden auch nahe liegende Themen wie der Aufbau von vermaschten Funknetzen und Gateways für WLANs behandelt.

Dieses Seminar vermittelt unter anderem:

- ✓ Eigenschaften der verschiedenen Standards im WLAN Bereich
- ✓ Zugriff auf Funknetze
- ✓ Einfache Schutzmaßnahmen
- ✓ Angriffstechniken
- ✓ Erweiterte Authentisierung und Verschlüsselung
- ✓ Ausblick auf neuere Technologien

Themenauswahl

▲ Funknetzstandards

- IEEE 802.11 a|b|g • IEEE 802.1X
- Eigenschaften • Stärken und Schwächen

▲ Hardware

- PCI/PCMCIA Karten • Antennen
- GPS • Embedded Systems
- Access Points und Router

▲ Software

- Integration in unterschiedliche Betriebssysteme • Wireless Tools

▲ Hacking

- Netstumbler • Ministumbler
- Ethereal • Kismet • Wellenreiter
- WEP Crack • Fälschen von Access Points

▲ Schutzmaßnahmen

- Basisabsicherung
- Authentisierung • Radius, X509
- WEP • WPA • WPA2 • IPSEC
- TKIP

▲ Komplexe WLAN Infrastruktur

- Mesh Protocol • Einsatz intelligenter Access Points
- Einsatz von WLAN Gateways
- Integration in bestehende Netzwerkinfrastruktur

▲ Ausblick

- Neue Standards • Erweiterte Integration in Betriebssysteme

Zielgruppe

- IT-Leiter • Netzwerk- und Systemadministratoren

Voraussetzungen

- Gute Kenntnisse gängiger Betriebssysteme
- Grundlegende Netzwerkkenntnisse

Dauer

3 Tage

Maximalzahl Teilnehmer

8

Preis

EUR 1.290,00 zzgl. MwSt.

Termine

09.05. – 11.05.2011

21.09. – 23.09.2011

12.12. – 14.12.2011

Ort

München

Auch jederzeit Inhouse möglich



▲ Teilnahme

Die Auswahl der gewünschten Veranstaltung liegt beim Teilnehmer, der die notwendigen Voraussetzungen mit seiner Anmeldung anerkennt.

Die jeweilige Veranstaltung wird nach heutigem Stand der Technik sorgfältig vorbereitet und durchgeführt. Beratungen zur Teilnahme und den Teilnahmevoraussetzungen seitens des Teilnehmers sind unverbindlich.

▲ Anmeldung

Die Anzahl der Teilnehmer an den Trainings und Workshops der GENIA-SEC GmbH sind begrenzt. Anmeldungen können nur 14 Tage vor dem geplanten Termin entgegengenommen werden, wobei die Reihenfolge des Eingangs der Anmeldung berücksichtigt wird.

Ein Vertrag kommt erst durch die Auftragsbestätigung der GENIA-SEC GmbH zustande.

▲ Teilnahmegebühr

Sämtliche Preise verstehen sich pro Teilnehmer, sind in Euro angegeben und verstehen sich zzgl. der gesetzlichen Mehrwertsteuer. Die Teilnahmegebühr ist vor dem Beginn der Veranstaltung auf das auf der Rechnung angegebene Konto zu zahlen. In der Teilnahmegebühr sind sämtliche Unterlagen sowie die Pausenverpflegung enthalten.

▲ Stornierung

Bei der Absage einer verbindlich bestätigten Teilnahme fällt bis zwei Wochen vor Beginn der Veranstaltung eine Bearbeitungsgebühr von € 50,- an. Erfolgt die Stornierung bis eine Woche vor Beginn der Veranstaltung, ist die halbe Seminargebühr fällig. Erfolgt die Stornierung noch später oder erscheint der Teilnehmer nicht, wird die volle Gebühr berechnet. Ersatzpersonen werden von GENIA-SEC GmbH selbstverständlich akzeptiert.

▲ Vorbehalte

GENIA-SEC GmbH behält sich vor, Veranstaltungen aus organisatorischen oder anderen Gründen abzusagen. In diesem Fall werden angemeldete Teilnehmer umgehend benachrichtigt und bereits gezahlte Gebühren erstattet. Weitere Ansprüche bestehen ausdrücklich nicht.

▲ Weiteres

Die im Rahmen der Veranstaltung überreichten Unterlagen obliegen dem Copyright, so dass hiervon keine Kopien angefertigt oder sie Dritten überlassen werden dürfen.

Mit der Anmeldung werden die oben genannten Bedingungen akzeptiert.

Für Rückfragen steht Ihnen das Team von GENIA-SEC GmbH gerne zur Verfügung:

GENIA-SEC IT-Sicherheitsmanagement GmbH
Lerchenstr. 40
D-86830 Schwabmünchen
Telefon: +49 (8232) 730 221
Telefax: +49 (8232) 730 227
E-Mail: info@genia-sec.de

Anmeldung



▲ Per Fax an +49 (8232) 730 227

Hiermit melde ich mich verbindlich für folgende(s) Training(s) an:

Titel des Trainings	Termin/Ort	Code	Kursgebühr

Meine persönlichen Daten:

<i>Name, Vorname</i>	
Funktion/Abteilung	
Firma	
PLZ, Ort	
Straße	
Telefon	
Telefax	
E-Mail	

Geben Sie hier bitte eine ggf. abweichende Rechnungsanschrift an:

Ort, Datum

Unterschrift

Tagungsunterlagen, Pausengetränke und Mittagessen sind in den Kursgebühren (zzgl. MwSt.) enthalten. Den Teilnahmebedingungen stimme ich durch meine Unterschrift zu.