



## Kursabstract für Kurs LAB-WS Wireless Security

Subject	Beschrieb
Kursdauer	1 Tag
Zielgruppe	<ul style="list-style-type: none"><li>✦ Security Officers</li><li>✦ Security Engineers</li><li>✦ Netzwerk Spezialisten</li><li>✦ Mobilkommunikation Spezialisten</li></ul>
Voraussetzung	<ul style="list-style-type: none"><li>✦ Vertrautheit mit der Windows Kommandozeile</li><li>✦ Vertrautheit mit der bash (Unix Prompt)</li><li>✦ Router, Switch, TCP/IP und Ethernet sind bekannte Begriffe</li></ul>
Inhalt	<ul style="list-style-type: none"><li>✦ Einführung in Wireless Netzwerke und Perimeter Sicherheit</li><li>✦ Angriffe gegen VPNs</li><li>✦ Angriffe gegen Wireless LANs (WEP, WPA und WPA2)</li><li>✦ Angriffe gegen Bluetooth Geräte</li><li>✦ Angriffe gegen DECT Telefonesysteme</li><li>✦ Ortung, Überwachung und Umleitung von Mobiltelefonen</li><li>✦ Fälschen von Kurznachrichten</li><li>✦ Diskussion zu Abwehrmassnahmen und möglichen weiteren Gefahren</li></ul>
Lernziel	Der Teilnehmer kann nach dem Kurs Schwachstellen im eigenen Unternehmen aufdecken und weiss, wie diese zu beheben sind. Er kann Massnahmen für den sicheren Betrieb der gängigen Wireless Technologien umzusetzen und kennt die Risiken.
Abgrenzung	Der Kurs ist auf Wireless Netzwerke und Mobilkommunikation fokussiert. Nessus, Nmap und Vulnerability Scanning sind nicht Bestandteile dieses Kurses (diese Themen werden im Kurs LAP-NP vermittelt).