
Dienstleistungs-Spezifikation

Sicherheit im Umfeld von Wireless LANs

„Sicherheit ist ein Prozess, kein Produkt.“

Bruce Schneier, Kryptologe und Sicherheitsberater

Die Sicherheit von Wireless-LAN-Systemen nach dem Standard IEEE802.11 schien dank WEP (Wired Equivalent Privacy) bis vor kurzem der von drahtgebundenen LANs kaum nachzustehen. Gerade in den letzten Monaten ist diese Sicherheit gegen fremdes Eindringen vollständig in Frage gestellt worden. Es sind Schwachstellen sowohl in den grundlegenden Protokollen, Übertragungs- und Verschlüsselungsverfahren, als auch in im Handel befindlichen Geräten und installierten Systemen, gefunden und publiziert worden.

Die Sicherheit von WEP allein ist nicht mehr gegeben

Werkzeuge, mit denen WEP-Keys in wenigen Minuten bis Stunden gebrochen werden können, sind frei verfügbar. Die Konstruktion von Einbruchswerkzeugen ist für den routinierten Hacker ein Kinderspiel. Erleichtert wird dies durch im Quellcode frei verfügbare Treiber für die meisten WLAN-Karten.

Viele Hersteller von WLAN-Systemen haben nicht geschlafen und eine Reihe von Verbesserungen in ihre Systeme eingebaut. Einige davon fließen gegenwärtig in den neuen Sicherheitsstandard für WLAN-Systeme IEEE802.11i ein. Diese Verbesserungen erlauben, WLANs wieder ähnlich sicher zu machen, wie drahtgebundene LANs. Doch auch Maßnahmen, die ein System heute praktisch sicher machen, können, durch neue Erkenntnisse der Kryptologie oder durch die simple Entdeckung von Systemfehlern, morgen schon überholt sein. Und manche neuen Sicherheitstechnologien stellen sich als bloße Marketingmaßnahmen heraus.

Systemadministratoren sind gefordert

Bei dieser rapiden Entwicklung von Technologien, Bedrohungen und Gegenmaßnahmen ist es für Anwender von Wireless LANs selbst mit hohem Aufwand kaum möglich, dem Stand der Technik zu folgen und möglichen Angreifern stets ein entscheidendes Stück voraus zu bleiben. Die rasante Verbreitung von Internet-Würmern wie Nimda liegt nicht darin begründet, dass die Schwachstellen in Systemen, die sie ausnutzen, neu und unbekannt sind. Vielmehr fehlt den

Administratoren häufig das Know-How oder einfach die Zeit, alle notwendigen Maßnahmen zur Sicherung ihrer Systeme, z.B. durch Einspielen von Bug-Fixes der Hersteller, zu ergreifen.

Wir beherrschen den Prozess Sicherheit

eMNetCon befasst sich primär mit WLAN-Technologie und verfolgt intensiv alle Entwicklungen in Bezug auf die Sicherheit der WLAN-Standards. Darüber hinaus arbeiten wir eng mit Anbietern zusammen, um die Tauglichkeit von Sicherheitslösungen für die Praxis zu prüfen und zu optimieren. Unsere daraus erwachsende Erfahrung bei der Sicherung von WLAN-Systemen steht auch Ihnen zur Verfügung.

Die Leistungen von **eMNetCon** im Detail

- ✓ Beratung zu allen Fragen der Sicherheit von drahtlosen LANs
- ✓ Analyse und praktische Überprüfung der Sicherheit bestehender Systeme durch Schwachstellenanalyse und gezielte Tests
- ✓ Entwicklung von Sicherheitskonzepten für Netzwerke und IT-Systeme
- ✓ Planung der notwendigen technischen und organisatorischen Sicherheitsmaßnahmen
- ✓ Installation und Konfiguration von Sicherheitskomponenten wie:
 - ✓ Firewalls und Paket-Filtern auf Routern
 - ✓ Access-Controllern z.B. auf Basis von IEEE 802.1x, Radius und Kerberos
 - ✓ Virtual Private Networks im WLAN
- ✓ Aktivierung aller vorhandenen Sicherheitsmechanismen in existierenden Systemen, z.B.:
 - ✓ SSID und Passwörter
 - ✓ Paketfilter und ACLs in Access-Points
 - ✓ WEP mit Shared Keys
- ✓ Verbesserung der physikalischen Sicherheit von WLANs durch präzisere Funkausleuchtung und Abschirmung unerwünschter Abstrahlungen
- ✓ Schulung von Anwendern und Systemspezialisten in Fragen der Systemsicherheit

**Für weitere Informationen stehen wir Ihnen gerne zur Verfügung.
Bitte rufen Sie uns an!**



eMNetCon Netzwerk Consulting GmbH

Cordt-Buck-Weg 45g
D-22844 Norderstedt

Tel./Fax: +49 700 EMNETCON (+49 700 36638266)

Internet: www.emnetcon.de
E-Mail : info@emnetcon.de