

## Notebooks und PDAs mit WLAN-Karten oder Bluetooth-Adaptern sind Ziele von Hackern

### cirosec bietet innovative Produkte zur Erkennung und Verhinderung von Angriffen per Funk

HEILBRONN, 13. September 2004 – cirosec, der Spezialist im IT-Sicherheitsbereich weist auf Sicherheitsrisiken durch moderne Notebooks hin. Neue Notebooks enthalten heute bereits alle benötigten Komponenten, um sie an Funknetze anzuschließen oder um per Bluetooth Daten mit dem Handy oder dem PDA auszutauschen. Auch wenn der Besitzer selbst keine Wireless LANs einsetzt, können diese Features oft von Hackern ausgenutzt werden, um über Funk unbemerkt in das Notebook einzubrechen, die dort gespeicherten Dateien zu stehlen oder um das Notebook als Hintertüre in Unternehmensnetze zu missbrauchen.

Als Lösung für diese Probleme ist cirosec eine Partnerschaft mit dem Wireless-Security-Spezialisten AirDefense eingegangen. Mit dem Produkt von AirDefense kann man rund um die Uhr alle Wireless-Aktivitäten im „Luftraum“ um das Firmen-Gelände in Echtzeit überwachen und bei erkannten Angriffen automatisch Gegenmaßnahmen einleiten.

Für Firmen, die sich bisher mit der Sicherheit von Funknetzen beschäftigt haben, war meist der wichtigste Aspekt, dass Hacker möglicherweise in das firmeneigene Funknetz eindringen könnten. Verhindert werden sollte dies mit Hilfe von starken Verschlüsselungs- und Authentisierungs-Verfahren. Berichte in den Medien über so genannte „War Driver“, die mit einer großen Antenne auf dem Auto durch die Straßen fahren, um ungesicherte Funknetze zu finden, haben dieses unvollständige Bild in der Öffentlichkeit verstärkt.

Tatsächlich sind von der Einbruchgefahr jedoch auch Organisationen betroffen, die selbst gar keine Funknetze betreiben und die sich mit diesem Thema bisher auch nicht beschäftigt haben. Das Problem sind moderne Notebooks nahezu aller Hersteller, die mit eingebauten Funk-Adaptern für Wireless LAN oder Bluetooth ausgeliefert werden und die verstärkt das Ziel von Angreifern sind.

Eine falsche Konfiguration, versehentliches Aktivieren der WLAN-Funktion durch Tastendruck oder die vergessene Deaktivierung der WLAN-Funktion nach dem Surfen in der Flughafen-Lounge machen das Notebook zu einem leichten Opfer. Der Angreifer täuscht dazu entweder einen Access Point unter falschem Namen vor, mit dem sich das Notebook automatisch verbinden kann oder er verwendet die Funktionen zur direkten Rechnerkopplung über WLAN.

Ähnliche Möglichkeiten existieren bei Notebooks mit eingebauten Bluetooth-Funktionen. Erst kürzlich veröffentlichten die einschlägigen Mailing-Listen Meldungen über Puffer-Überläufe in der Bluetooth-Treiber-Software, die in der Mehrzahl aller Notebooks verwendet wird. Durch diese Verwundbarkeiten können Angreifer die Kontrolle über das betroffene Notebook erlangen. Sofern die modernen Notebooks innerhalb eines Firmennetzes angeschlossen werden, können die Funk-Adapter zu einer Hintertüre in das Firmennetz werden. Das Notebook wird dabei zum Gateway zwischen den Funk-Signalen des Angreifers und dem normal verkabelten Firmennetz.

Die klassischen Gegenmaßnahmen wie VPN-Verschlüsselung im WLAN und starke Authentisierung sind bei diesen Problemen nutzlos, da es sich nicht um Angriffe auf ein offiziell aufgebautes WLAN handelt, sondern um Angriffe über unbeabsichtigte Features



cirosec GmbH  
Ferdinand-Braun-Straße 3  
74074 Heilbronn  
Tel.: 07131 / 59455-60  
Fax: 07131 / 59455-99  
[www.cirosec.de](http://www.cirosec.de)

in Notebooks. Interessant in diesem Zusammenhang: Im Gegensatz zur weit verbreiteten Meinung, dass Bluetooth nur im Umkreis von zehn Metern funktioniert, hat eine Hacker-Gruppe im August nachgewiesen, dass mit geeigneten Antennen ein Angriff sogar aus einer Entfernung von einem Kilometer durchgeführt werden kann.

Die Lösung von AirDefense besteht aus einer Management-Station und verschiedene Funk-Sensoren. Die Sensoren beobachten rund um die Uhr alle Wireless-Aktivitäten und melden diese an die Management-Appliance. Die Appliance korreliert und analysiert die Daten dann nach Schwachstellen und Netzwerkbefindlichkeiten. Dabei wird die Einhaltung der Policy kontrolliert, die Signaturen werden analysiert und anomales Verhalten aufgedeckt. Illegale Aktivitäten, unerlaubte oder vorgetäuschte Access-Points oder andere Angriffe über Funk sind ebenso ersichtlich, wie die aktuellen erlaubten Funk-Verbindungen und der Status der einzelnen Stationen und Access-Points. Ebenso kann die Einhaltung von Security Policies kontrolliert werden oder die Verfügbarkeit gewährleistet werden. Bei erkannten Angriffen können sogar automatisch Gegenmaßnahmen eingeleitet werden. Auf diese Art und Weise ist mit der Technologie von AirDefense eine genaue Darstellung der Sicherheitsrisiken, aber auch der Netzwerk-Performance möglich.

#### Über AirDefense

Founded in 2001, AirDefense™ is the thought leader and innovator of wireless LAN security and operational support solutions. AirDefense has pioneered the concept of 24x7 monitoring of the airwaves and now with thirteen patents pending, helps enable risk-free wireless LANs for organizations. AirDefense provides the most advanced solutions for enterprise wireless LAN security, policy, enforcement & operational support. As a key element of wireless LAN security, AirDefense complements wireless VPNs, encryption and authentication. The solution works with any vendor, any protocol and any device.