



## PCI-Compliance – Kurzbeschreibung

Am Freitag, dem 4. Mai 2007, als das Wall Street Journal auf der Titelseite einen Bericht über eine Sicherheitslücke im WLAN-Bereich veröffentlichte, die zum größten Kreditkartenbetrug aller Zeiten führte, wurde der schlimmste Alptraum eines jeden Einzelhändlers wahr. Die PCI-Vereinigung, die sich aus den fünf wichtigsten Kreditkartenunternehmen – American Express, Visa, Mastercard, Discover und JCB – zusammensetzt, entwickelte den Payment Card Industry Data Standard (PCI DSS), um genau solche Sicherheitslücken zu schließen. PCI verlangt von Einzelhändlern weltweit, Drahtlosnetzwerke als öffentliche Netze zu definieren und entsprechend strikte Maßnahmen einzuführen. Dies gilt für die Bereitstellung von Anwendungen über WLAN. Außerdem sollen drahtlose Netzwerke vor unautorisierten Übergriffen geschützt werden.

Die Einhaltung der PCI-Richtlinien ist jedoch kompliziert und teuer. Bereits bestehende kabelgebundene und drahtlose Netzwerke müssen aktualisiert, zusätzliche Sicherheitsdienste müssen installiert werden. Das kann schnell zu einer kostspieligen und entmutigenden Angelegenheit werden, besonders wenn es um Hunderte oder gar Tausende von Geschäften geht. Mit benutzerzentrierten Netzwerken von Aruba steht die einzige Lösung bereit, die hohe Sicherheit, WLAN und Remote-Zugang integriert, um eine PCI-Zertifizierung so reibungslos und kosteneffektiv wie möglich zu gestalten. Aruba bietet eine zentral verwaltete Sicherheitslösung, die auf der Grundlage bereits bestehender Netzwerke funktioniert. Damit sind Neu-Design und Aktualisierung nicht notwendig. Darüber hinaus unterstützt die Plattform weitere Anwendungen. Dieselbe Lösung, die Ihre Sicherheitsprobleme löst, unterstützt auch bestehende und neue WLAN-Anwendungen.

## PCI-Anforderungen für die Sicherung von Drahtlosnetzwerken

Die PCI-Vereinigung veröffentlichte im Mai 2006 eine aktualisierte Version ihres Data Security Standards (DSS), die seit dem 1. Januar 2007 in Kraft ist. Die PCI sieht die Einbindung spezieller Sicherheitskontrollen vor, die sich je nach dem Gebrauch drahtloser Netzwerke unterscheiden.

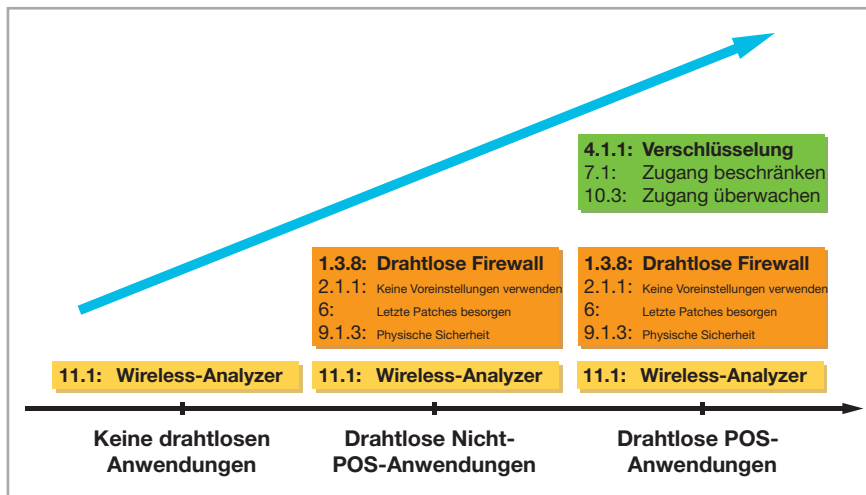
Selbst wenn keine Drahtlosnetzwerke verwendet werden, müssen „Wireless-Analyzer“ integrieren sein, die vor unbeabsichtigten oder nicht autorisierten Drahtlosnetzwerke schützen.. Falls Einzelhändler Drahtlosnetzwerke jedoch für Point-of-Sale-Anwendungen einsetzen und Kreditkartendaten drahtlos übertragen werden, müssen sie eine leistungsfähige Verschlüsselung (nicht WEP) sowie eine ICASA-zertifizierte Firewall zwischen WLAN und POS-Netzwerk verwenden und darüber hinaus den WLAN-Datenverkehr regelmäßig überwachen.

PCI-Compliance hat höchste Priorität. Da PCI-Compliance die Sicherung Ihrer Netzwerke bedeutet, schützen Sie dadurch gleichzeitig Ihre Marke und Ihre Kunden. Darüber hinaus haben sich die Kreditkartenunternehmen auf zusätzliche Anreize zur Beschleunigung der PCI-Zertifizierung geeinigt. Dazu gehören:

- Kaum Strafen von bis zu 25.000 US-Dollar pro Laden pro Monat bei Nicht-Zertifizierung
- Qualifizierung für bevorzugte Transaktionsraten
- Schutz im sicheren „PCI-Hafen“, indem PCI-zertifizierte Einzelhändler weder haftbar gemacht werden können noch die im Falle eines Datendiebstahls übliche Strafe von etwa 160 US-Dollar pro gestohlenem Kreditkartensatz zahlen müssen.

### Die Aruba-Vorteile:

- Niedrige TCO mit integrierter Sicherheit für PCI-Compliance
- Schutz bereits vorhandener Netzwerke durch Overlay-Architektur
- Vermeidung von Upgrades von nur WEP-fähigen Geräten dank identitätsorientierter Sicherheitsmechanismen
- Einfache Migration zu Drahtlosnetzwerken der nächsten Generation mit Mehrzweckplattform
- Ausrichtung auf die Skalierbarkeit viele Remote-Einzelhandelsfilialen

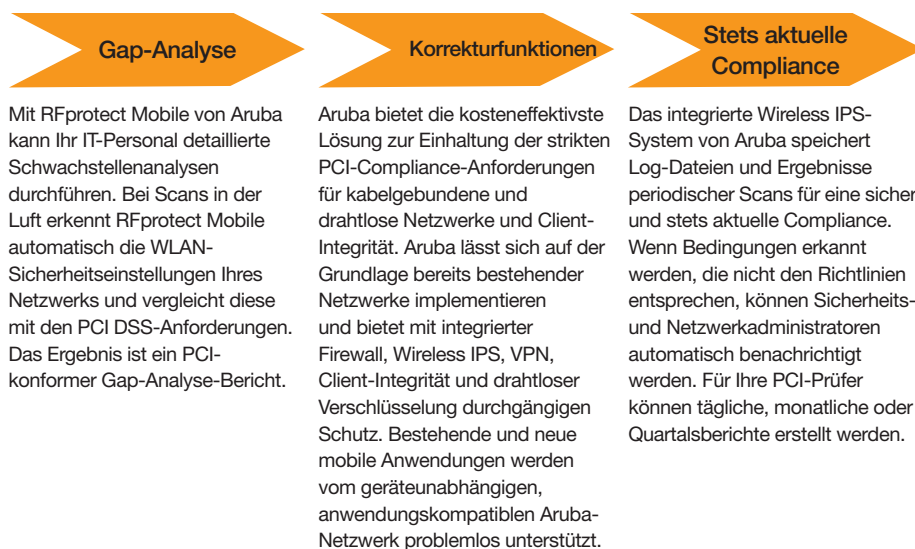


## Der Weg zur PCI-Compliance – die Lösung von Aruba

Aruba Networks hat einen einzigartigen Ansatz entwickelt, die PCI-Anforderungen kosteneffektiv zu erfüllen. Dank einer Lösung, die hohe Sicherheit, kabelgebundene, drahtlose Netzwerke und Remote-Zugang integriert, können Einzelhändler die für PCI-Compliance erforderlichen Sicherheitsmechanismen ohne ein Upgrade der bisherigen Netzwerke in Kraft setzen und Geschäftsanwendungen implementieren. Eine detaillierte Beschreibung der Aruba-Lösung für PCI-Compliance finden Sie

unter: [http://www.arubanetworks.com/pdf/company/wp\\_PCI-Primer.pdf](http://www.arubanetworks.com/pdf/company/wp_PCI-Primer.pdf).

Aruba bietet eine End-to-End-Lösung, die die PCI-Compliance Ihres Drahtlosnetzwerks gewährleistet und die – was noch wichtiger ist – Ihr Netzwerk rundum schützt. Ob Gap-Analysen zur Erkennung potentieller Sicherheitslücken, Korrekturfunktionen oder Überwachungs- und Prüffunktionen – für alle Bereiche bietet Aruba die geeignete Lösung an.



**PCI-SICHERHEIT MIT EINFACHER IMPLEMENTIERUNG:**

Funktionen wie Wireless Intrusion Protection Services (IPS) können innerhalb bestehender Netzwerkinfrastrukturen implementiert werden. Die Lösung von Aruba sieht einen (oder mehrere) Air Monitor(e) in den Läden sowie einen Wireless Intrusion Protection-Server im Datenzentrum vor. Air Monitore führen kabelgebundene und drahtlose Scans der Ladenumgebung durch. Zentralisierte Server stellen die Scan-Daten dann zusammen und analysieren sie. Über die so generierten PCI-Scan-Berichte wird die Compliance sichergestellt. Im Falle eines nicht autorisierten Zugriffs generiert das Wireless IPS-System Alarme und verhindert automatisch mögliche Angriffe. Die Aruba-Lösung ist deswegen einzigartig, weil dieselbe Hardware, die für Wireless IPS verwendet wird, auch für drahtlosen Zugang konfiguriert werden kann und deswegen einen einfachen und kosteneffektiven Weg zur nächsten Generation von Drahtlosnetzwerken darstellt.

**KEINE UNNÖTIGEN NETZWERKUPGRADES UND NEUDESIGNS:**

Mit den integrierten Bestandteilen der Lösung von Aruba wie ICSA-zertifizierter Stateful-Firewall, VPN und WLAN-Authentifizierung/-Verschlüsselung brauchen bestehende kabelgebundene Netzwerkprodukte wie Router und Firewalls nicht für VLAN-Unterstützung, VPN-Fähigkeit oder AAA-Dienste für drahtlose Sicherheit aktualisiert zu werden.

**SCHUTZ VON NUR WEP-FÄHIGEN GERÄTEN DURCH IDENTITÄTSORIENTIERTE SICHERHEIT:**

Mit den auf Gerät und Benutzer basierenden Sicherheitsrollen von Aruba können Sie verhindern, dass nur-WEP-fähige Geräte in Ihr Datenzentrum eindringen. Selbst bei einer Kompromittierung der WEP-Verschlüsselung wird der Zugang zum Netzwerk über die integrierte, tief reichende Paketanalyse (DPI - Deep Packet Inspection) und die Stateful-Firewall begrenzt.

**EINE PLATTFORM, VIELE MÖGLICHKEITEN:**

Zusätzlich zu allen Sicherheitsfunktionen bietet die Lösung von Aruba gesicherte Konnektivität für drahtlose, kabelgebundene und vermaschte Netzwerke der Enterprise-Klasse, die für viele Anwendungen verwendet werden kann. Dazu gehört u. a. die gleichzeitige Unterstützung für Daten, Sprache und Video auf einem beliebigen Gerät.

**ZENTRALE VERWALTUNG:**

Aruba bietet je nach Ladengröße unterschiedliche Optionen, die alle zentral als ein einziges Netzwerk verwaltet werden können. Bei der Entwicklung der Aruba-Lösung war die Sicherheit privater und öffentlicher Netze ein wichtiges Kriterium. Die Richtlinien für Tausende von Remote-Standorten werden dabei zentral definiert und ihre Einhaltung überwacht.



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550