



COMPUTERWORLD

November 15, 2007

What retail wireless security? TJX has plenty of company in the blithe-indifference pool

By Jaikumar Vijayan

November 15, 2007 (Computerworld) -- TJX may be in a class all by itself in terms of the number of records compromised in a data breach. But the retailer apparently has plenty of company when it comes to wireless security issues of the sort that led to the compromise it disclosed earlier this year.

A survey of over 3,000 retail stores in several major U.S. cities by wireless security vendor [AirDefense](#) Inc. reveals that a large number of retailers are failing to take even the most rudimentary steps for protecting customer data from wireless compromises.

Among the biggest issues: weakly protected client devices, wrongly configured wireless access points inside stores, data leakage, poorly named network identifiers, and outdated access-point firmware.

According to [AirDefense](#), about 85% of the 2,500 wireless devices that it discovered in retail stores, such as laptops and barcode scanners, were vulnerable to wireless hacks. Out of the 4,748 access points that were monitored for the survey, about 550 had poorly named SSIDs that could give away the store's identity.

"One thing we did not expect was the large number of point-of-sale devices that looked as if they had been turned on" and left in essentially the configuration in which they arrived at the store, said Richard Rushing, chief security officer at [AirDefense](#). Many of the access IDs that were being used by retailers had names that were dead giveaways, such as 'retail wireless', 'POS WiFi' or 'store number 1234'," Rushing said. "I can guarantee that all of these stores were also using default configurations" on their access points, he said. "You really are knocking at the doors of hackers," with such weak security practices, he said.

About 25% of the access points that were monitored used no encryption at all. In total, of the 3,000 stores monitored, about a quarter of them were still using the Wired Equivalent Privacy (WEP) protocol for encrypting traffic. WEP is considered to be among the weakest of the encryption options available today and was the standard in use by TJX when it was first breached.

In at least a few cases, Rushing said, stores were using legacy protocols that many companies have stopped using for some time now.

Among such legacy protocols were Novell's IPX, Banyan Vines and IBM's SNA , he said, "This is stuff we simply did not expect," he said. "Some of this has been banished from corporations for years," he added.

The findings in the AirDefense survey are not at all surprising, even if they're from a vendor that sells wireless security products, said Avivah Litan, an analyst with Gartner Inc. in Stamford, Conn.

"Certainly vendors are trying to promote their products," with surveys that highlight the need for their products, Litan said, At the same time, the AirDefense study only bolsters what others have been also saying for some time now, she said.

"Wireless security continues to be the major hole that allows criminals access to retailer systems," she said. "It's very difficult to lock it down" for retailers. Many are still not even sure of the sheer number or variety of devices hanging off their wireless networks nor how to look for them, and even the auditors who asses retailers for their compliance with the payment card industry data security standard (PCI-DSS) mandated by the credit card companies sometime miss wireless weaknesses, she said.

Despite continuing stumbles, retailers in general are becoming more aware of wireless security issues said Cathy Hotka, president of Cathy Hotka & Associates, a retail consultancy in Washington. Until fairly recently, for instance, it wasn't at all unusual for store managers to install their own wireless gear at their locations. "The security of the store was really up for grabs," back then she said. Similarly, during the holiday shopping rush, stores would routinely set up ad hoc point of sale systems, and other those too were poorly secured.

"That really isn't the case anymore," she said. "Companies are well aware of the wireless requirements for PCI," and have been trying to address it.